

**READY FOR TAKEOFF:
YOUR SOVEREIGN
CLOUD JOURNEY
STARTS HERE**



Picture generated
with AI

T Cloud

TABLE OF CONTENTS

1	How companies keep control over their data and infrastructure	Page 4
2	What you should know about digital sovereignty	Page 8
3	The right measures: How much digital sovereignty is sensible?	Page 11
4	Crucial: How to think cloud sovereignty strategically	Page 14
5	Functionality vs. sovereignty: A solution portfolio for every need	Page 18
6	Sovereign cloud platforms from Telekom at a glance	Page 20
7	How our sovereign cloud platforms ensure success	Page 24
8	Key learnings: The dos and don'ts of digital sovereignty	Page 28

DIGITAL SOVEREIGNTY OPENS UP OPPORTUNITIES FOR GROWTH AND INNOVATION

Dear readers,

We all know the advantages of the cloud: scalability, flexibility, and the ability to promote global collaboration through real-time access to data and applications. These benefits have transformed entire industries in recent years, enabling companies to innovate faster and work more efficiently.

However, not all organizations can fully harness the potential of the cloud. For example, public clouds are often unsuited to sectors such as healthcare, finance, and public administration, which store and process large volumes of sensitive data and must meet regulatory requirements. Concerns about data sovereignty and compliance with European laws such as the GDPR make the use of traditional public clouds problematic.

Multi-clouds for more digital sovereignty

These challenges are where T-Systems comes into play. Our ‘Made in Germany’ portfolio of competitively priced multi-cloud solutions ranges from feature-rich hyperscaler solutions to highly customized private and multi-cloud platforms. This way, you benefit from the flexibility and innovative power of the cloud while retaining complete control over your data in accordance with your specific needs.

Interested in learning more? Explore our e-book to see how our sovereign cloud solutions—crafted in Europe for Europe—protect your sensitive information and ensure your digital sovereignty.

Enjoy the read!



Dr. Christine Knackfuß-Nikolic
*Chief Technology Officer (CTO),
T-Systems International GmbH*

HOW COMPANIES KEEP CONTROL OVER THEIR DATA AND INFRASTRUCTURE

Which challenges can you overcome smoothly with a sovereign cloud?



Flexibility, scalability, and cost efficiency: the advantages of the cloud are numerous. However, not all organizations can benefit from them equally.

A public cloud's security and privacy measures are often inadequate for sectors such as healthcare, finance, or public administration, which manage sensitive data under strict regulatory requirements such as the GDPR or NIS2. Concerns over data sovereignty, data integrity, or vendor lock-in also argue against traditional public cloud solutions.

DIGITAL SOVEREIGNTY IN A NETWORKED AND SENSITIVE WORLD – A STRATEGIC NECESSITY

U.S. hyperscalers such as Amazon Web Services, Microsoft Azure, and Google Cloud hold over 70 percent of the market share¹ in the European cloud market. They not only set technological standards, but also influence the economic and legal conditions under which their European customers operate. Moreover, it is often unclear where some cloud providers, especially hyperscalers, store or process data. The risk is that sensitive company and customer information from Europe could leak. For privacy reasons alone, this compromises European companies by exposing them to potential data breaches.

Europe's path to a sovereign cloud future

Companies and government institutions face the challenge of finding the optimal solution for their data and various workload types while fully leveraging the potential of the cloud, with:

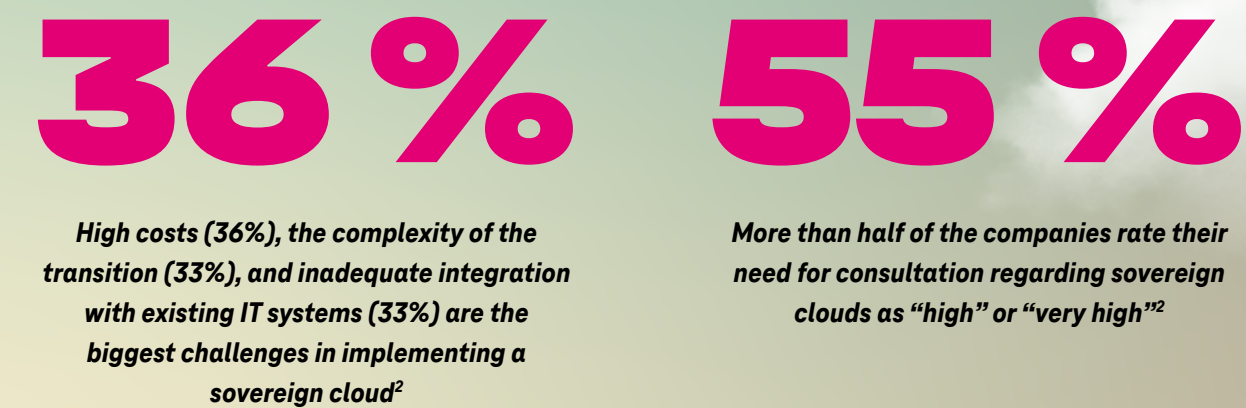
- High functionality and scalability
- Little cost
- Maximum sovereignty and security

A sovereign cloud helps achieve all three goals. It offers high functionality and the scalability of a modern cloud infrastructure whilst efficient resource utilization also helps minimize IT costs.

Digital sovereignty is far more than a technical buzzword – it is a strategic necessity in an increasingly interconnected and geopolitically sensitive world. Digitally sovereign companies, organizations, and states aim to exercise control over their digital infrastructures, data, and technologies independently and sustainably – without being dependent on third parties that may limit their decision-making and operational capabilities.

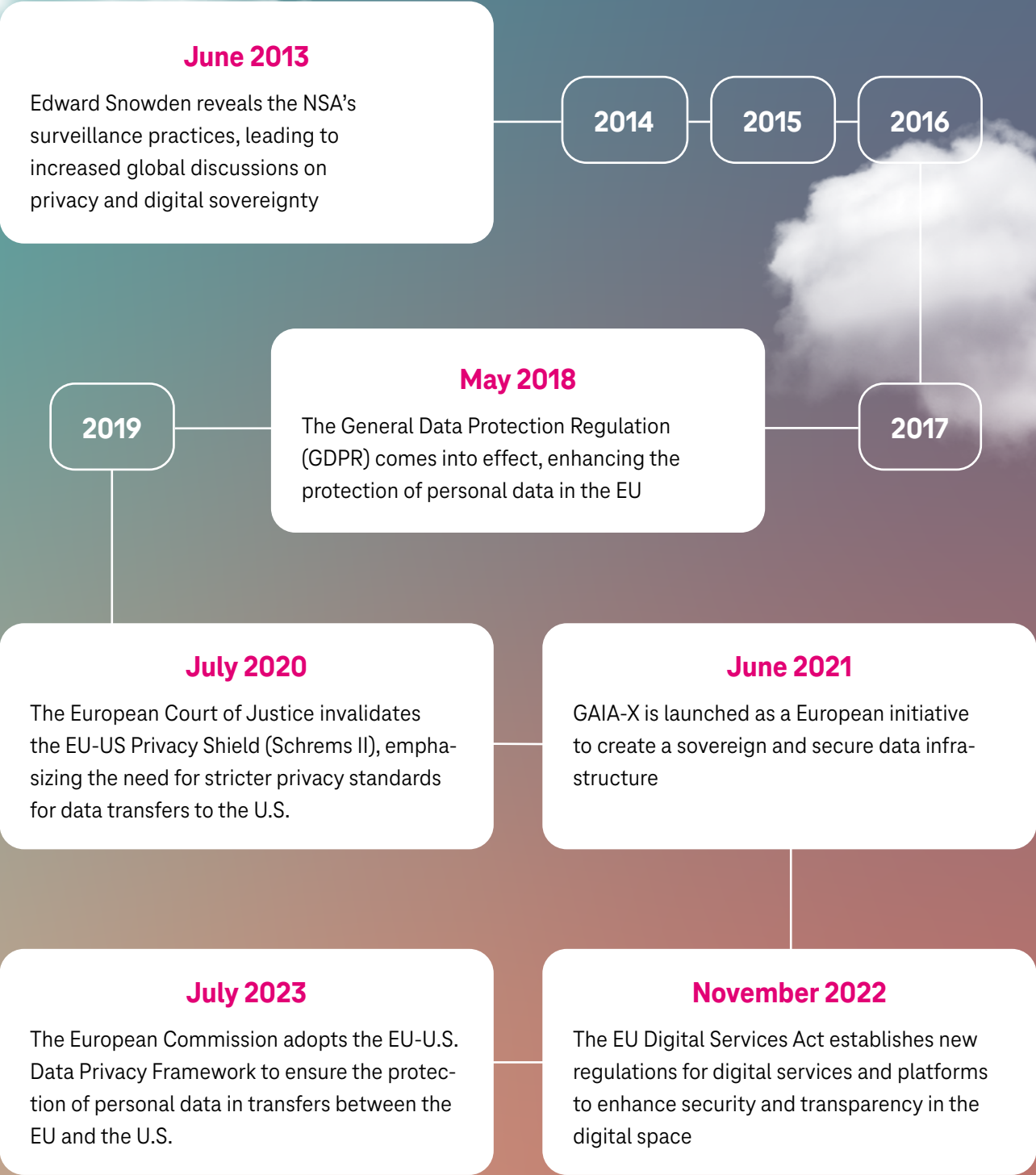
FACTS AND FIGURES

SOVEREIGN CLOUD:
EXTREMELY POPULAR,
RARELY USED



A JOURNEY THROUGH TIME

SIX MILESTONES OF
DIGITAL SOVEREIGNTY



WHAT YOU SHOULD KNOW ABOUT DIGITAL SOVEREIGNTY

The pillars of digital sovereignty:
Data, operations, and technology.



Digital sovereignty can be divided into three key areas: data sovereignty, operational sovereignty, and technology sovereignty. These levels are built upon each other and form the foundation for digital resilience and independence.

LEVEL 1: Data sovereignty

Data-sovereign organizations are always autonomous regarding their own data and ensure secure access. The risk arises when companies or authorities do not operate their own IT systems nor host their own data but instead rely on external IT service providers and cloud services. In these cases, it must be ensured that unauthorized parties are prohibited, that data is stored and processed according to applicable law, and that this law can be effectively enforced if necessary.

→ *Data sovereignty is the basis for trust – internally and externally – and is a prerequisite for any form of digital value creation*

LEVEL 2: Operational sovereignty

Companies and authorities must be independent from individual platforms when operating software and be free to decide where to run an application. Whether it be in their own data center, as a managed service with a self-selected IT service provider, or in a public cloud. The software itself must also ensure independence. Companies and authorities should be able to replace an application with an alternative solution at any time if needed. To do this, the software must support open standards that allow all types of data to be freely transferred to other systems without modification.

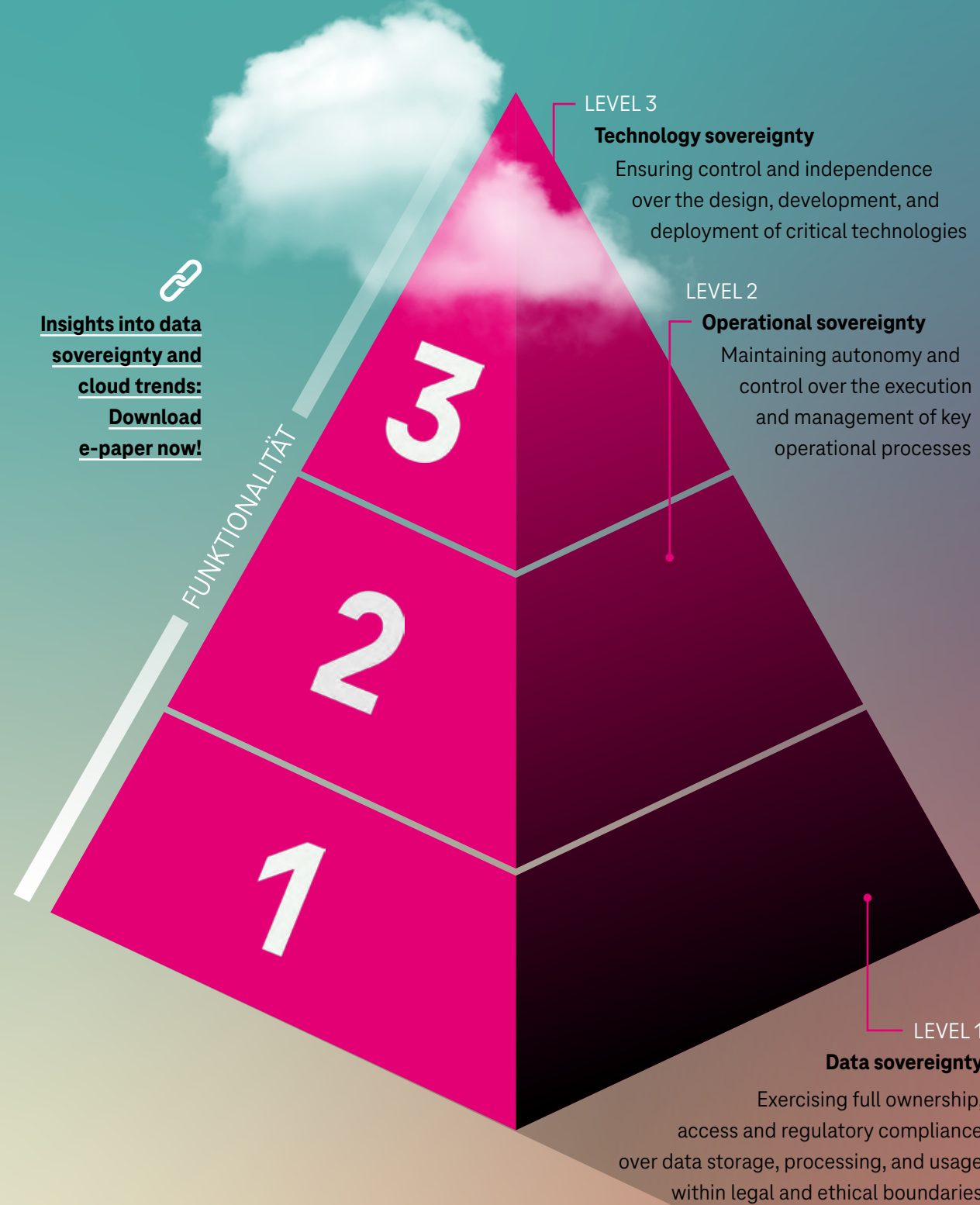
→ *A sovereign operation ensures that organizations remain independent and functional even in times of crisis or conflict*

LEVEL 3: Technology sovereignty

Organizations should be able to verify that software functions correctly. This is only possible if they have full transparency over the source code, through open-source or shared-source software. Open-source code allows companies and authorities to ensure software contains no backdoors through which data can surreptitiously reach third parties. Additionally, investments are protected: if the provider exits the market, they can continue to develop the software independently (with no vendor lock-in).

→ *Technology sovereignty creates room for innovation, strengthens digital resilience, and secures long-term competitiveness*

The three levels of sovereignty are essential



[Insights into data sovereignty and cloud trends: Download e-paper now!](#)

Start your sovereign cloud journey
How much digital sovereignty is sensible?

THE RIGHT MEASURES: HOW MUCH DIGITAL SOVEREIGNTY IS SENSIBLE?

A must for industries with the highest security requirements and strict regulations

Digital sovereignty plays an important role for certain companies and organizations. Sovereign clouds are essential when companies work with sensitive data, must meet regulatory requirements, or are part of critical infrastructures (KRITIS). This includes industries such as healthcare, the public sector, energy, finance, logistics, or security and defense. It's important to note, not every company needs to achieve the highest possible digital sovereignty. The required degree of sovereignty depends on various factors, such as the type of data, regulations, or specific business processes.

Different levels of digital sovereignty

For companies that do not process sensitive or regulated data, a cloud solution that meets basic security and privacy requirements while offering cost efficiency and scalability often suffices. An example would be an e-commerce provider that mainly manages customer data and needs to adhere to general security standards but does not handle highly sensitive information.

Other organizations require higher levels of sovereignty. For instance, universities and institutions managing large amounts of research data and personal information of students, must protect this data from unauthorized access and comply with privacy requirements such as the GDPR. At the same time, they need the flexibility and scalability of cloud solutions to meet the growing demands of digital education and research.



Digital Sovereignty as an innovation engine. Learn more in our blog article

For companies with critical infrastructures, such as hospitals, banks, energy providers, or logistics companies, a higher level of digital sovereignty is essential. These companies must not only implement strict security measures, but also ensure their operational processes continue uninterrupted in the event of a cyber-attack or geopolitical crisis. An energy company responsible for a country's power supply or a logistics provider managing the supply chain for essential goods must guarantee that their systems remain independent and functional at all times.

AI AND DIGITAL SOVEREIGNTY

AI systems require large amounts of data to function effectively. Digital sovereignty ensures that this data is processed securely and in accordance with applicable privacy regulations; without digital sovereignty, the use of AI is risky for companies. The data used for training and operating AI systems must be protected and should not be susceptible to misuse, transparency and control are crucial in the context of AI and all AI outcomes must be traceable and explainable. A black box with undocumented training data is unacceptable; companies should understand and control the decision-making processes of their AI systems, including knowing how AI algorithms work and what data they use.



DATA MANAGEMENT ESSENTIALS: DATA SOVEREIGNTY, DATA RESIDENCY, AND DATA INTEGRITY

DATA SOVEREIGNTY: synonymous with data sovereignty. Companies have full control over their data in the cloud, including storage location, access, security, and privacy.

DATA RESIDENCY: refers to the geographical location where the data servers are situated. The storage location is relevant because many countries have local data regulations that dictate where companies must collect, process, and store their data. For example, according to the GDPR, personal data of EU citizens must remain within the EU.

DATA INTEGRITY: requires a company's data is always accurate, complete, and consistent throughout its lifecycle. Therefore, the company must protect its data from loss, data leaks, and unauthorized access.

ACHIEVING DIGITAL SOVEREIGNTY CHECKLIST

To ensure digital sovereignty, companies should be able to satisfactorily answer the following questions:



PRIVACY UNDER GDPR: can your cloud provider guarantee that your data will not be transferred to different countries? Is all information consistently protected from access by foreign governments?



TRANSPARENCY AND CONTROL: How does your cloud provider ensure your data sovereignty? How dependent are you on your service provider for controlling your data?



DEPENDENCE ON HYPERSCALERS: What options do you have for customization and expansion? What opportunities are there for multi-cloud and hybrid strategies?



FUTURE SECURITY: Are you assured of receiving updates and security patches promptly and regularly? Could external actors prevent this?

4 CRUCIAL: HOW TO APPROACH CLOUD SOVEREIGN- TY STRATEGICALLY

Tailored advice for every sovereignty requirement:
How we support you on your journey to digital sovereignty

A successful cloud strategy requires an end-to-end approach that considers the entire IT landscape. No matter where you are on your cloud journey, we are here to support you. With our Cloud Professional Services, we build on business consulting and address your individual needs by jointly planning and implementing cloud transformation.


[Learn more about
Cloud Professional
Services from
T-Systems](#)

Our Sovereignty Advisory Services ensure that your cloud transformation meets all regulatory requirements and sovereignty goals. Whether you want to define new strategies, assess compliance, or create secure architectures, our experts help you build a compliant, stable, and future-proof environment. We evaluate your specific needs and guide you to the right level of sovereignty for your workload and use cases, whether it's integrating hyperscaler platforms—including managed services—or managing private cloud infrastructures as part of a seamless multi-cloud environment. In this way, we help you achieve exactly the digital sovereignty you need.

We advise: Strategy for cloud sovereignty

- Identification of sovereignty goals which consider business drivers and geopolitical context
- Impacts of GDPR, NIS2, EU Data Act, and non-EU legislation (e.g., US CLOUD Act)
- Definition of critical assets and creation of an initial roadmap for cloud sovereignty

We assess: Infrastructure, risk, and compliance

- Conducting a structured, multi-level assessment (compliance estimation, gap analysis, risk prioritization)
- Capturing the current state of infrastructure based on sovereignty standards (e.g., ISO 10866:2024)
- Providing clear, actionable compliance and risk reports

We review: Architecture and process blueprints

- Designing sovereignty-oriented architecture and operational models
- Recommending platform options or tailored architectural solutions
- Defining suitable governance models to support strategic sovereignty goals


Our strength:
Over 20 years of
cloud experience

We analyze: Optimal deployment of workloads

- Evaluating workloads based on data sensitivity, access control, and vendor dependencies
- Recommendations for the use of public, private, and sovereign clouds
- Advising on access governance and vendor compliance

WE HAVE THE IDEAL CLOUD FOR EVERY USE CASE

A statement from Gregory Hyttenrauch,
Senior Vice President Cloud Services at T-Systems

Companies today require flexible cloud strategies. Our customers have a wide range of different applications and use cases, which determine the right cloud solution. Not all workloads need a sovereign platform, yet businesses always need as much sovereignty as necessary even if they do not want to unnecessarily sacrifice innovation or functionality. With our expertise in sovereign solutions and our experience in managing multi-cloud environments, we are the perfect partner for this.

FACTS & FIGURES

T-SYSTEMS: OUR OPERATIONAL EXCELLENCE

~ 40.000

IT experts

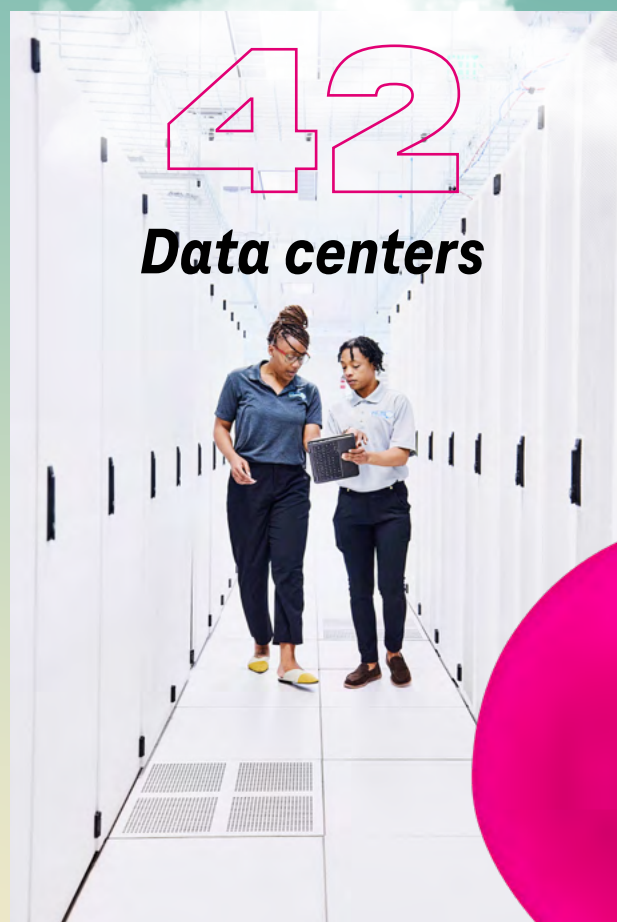


UP KKRITIS

Independent Partnership

42

Data centers



7.865

Patents



160

Official
open-source
repositories



5

FUNCTIONALITY VS. SOVEREIGNTY: A SOLUTIONS PORTFOLIO FOR EVERY NEED

Finding the optimal balance between functionality and security with a multi-cloud approach

A central theme in using sovereign clouds is the dilemma between functionality and sovereignty. While a variety of functions often presents higher risks, strong sovereignty offers more security but can limit speed and flexibility. Generally, functionality decreases as sovereignty increases.

Many companies face a dilemma in balancing functionality and scalability with sovereignty; T-Systems can help. We find the right balance between the necessary sovereignty and desired features, offering a broad portfolio tailored to all levels of sovereignty.



Readers' choice confirmed: T-Systems leads the way in sovereign clouds

Clear advantages of hybrid and multi-cloud

Companies can select cloud solutions tailored to their specific workloads and business goals through customized multi- and hybrid-cloud scenarios, avoiding a one-size-fits-all approach.

This strategy minimizes vendor dependence and allows leveraging the unique strengths of various offerings, leading to greater flexibility, independence, and optimal workloads. Hybrid integration enables companies to use global public cloud services for non-critical functions, while critical systems remain secure in sovereign environments.

T-Systems: sovereign cloud solutions for Europe

In the growing cloud market, T-Systems is the only provider offering the full spectrum of multi- and hybrid-cloud solutions, along with several sovereign cloud solutions—from fully independent sovereign clouds to scenarios developed in collaboration with hyperscalers. This unique approach allows our customers to choose the sovereignty level that best fits their business, regulatory, and operational requirements.

However, sovereignty comes at a price for several reasons: higher salaries are paid in German and European data centers than in many other regions, whilst Germany has higher energy costs. Certifications due to regulations are also costly. Not least, economies of scale are limited as sovereign clouds focus on specific regions.

WE OFFER THE FULL MULTI- AND HYBRID CLOUD SPECTRUM – SOVEREIGNTY FROM A SINGLE SOURCE

With over 20 years of experience in cloud and connectivity, including 14 years pioneering sovereign cloud solutions, we have the expertise to support you with industry-specific, secure solutions. As a German company deeply rooted in European values, we offer independence and security, ensuring you find the right balance between innovation and control.

OUR UNIQUE SELLING POINTS

Sovereign cloud, infrastructure, and end-to-end services from a single source. T-Systems can:

- provide the foundation for our customers' digitalization in a highly scalable, sovereign, secure, and sustainable manner
- implement operational excellence and offer premium products, which take care of all your needs
- offer hybrid and multi-clouds, including all levels of sovereignty, from a single source
- generate added value through customized solutions along the end-to-end stack including planning, installation, and operation
- provide a one-stop shop with everything required, from connectivity to security, cloud, and artificial intelligence (AI)

SOVEREIGN CLOUD PLATFORMS FROM TELEKOM AT A GLANCE

Customized cloud sovereignty
for your company

In addition to our Sovereignty Advisory Services described in Chapter 4, we offer several sovereign cloud platforms tailored to regulated industries, providing the highest security, compliance, and control.

Sovereign Controls by T-Systems

“Sovereign Controls” combine the technical Google Cloud Platform with sovereignty controls from T-Systems. With External Key Management, Access Controls & Transparency, Security Operations Center (SOC), and local support, T-Systems continuously monitors compliance with sovereignty requirements, making Google Cloud suitable for regulated industries.

AWS European Sovereign Cloud*

This solution is tailored to the sovereignty needs of the public sector and regulated companies. It will be operated independently from the global public cloud in the future, allowing customers to meet strict requirements for operational autonomy and data residency. Customers have control over where and how data is stored and who can access it.

OTC

Open Telekom Cloud (OTC) is the leading European public cloud of Deutsche Telekom, operated and managed by T-Systems. It is designed for Europe, regulated markets, and customers with high security and compliance requirements.

Hosted Cloud by T-Systems

This solution is based on Google Distributed Cloud – Air Gapped. It is an isolated cloud solution developed for highly regulated industries such as defense and finance, operating without web or Google Cloud connectivity, ensuring full data sovereignty and security compliance.

FCI

Future Cloud Infrastructure (FCI) is our comprehensive private cloud solution that accelerates your digital transformation and includes all necessary tools or APIs for self-management, supporting all critical business applications.

OSC

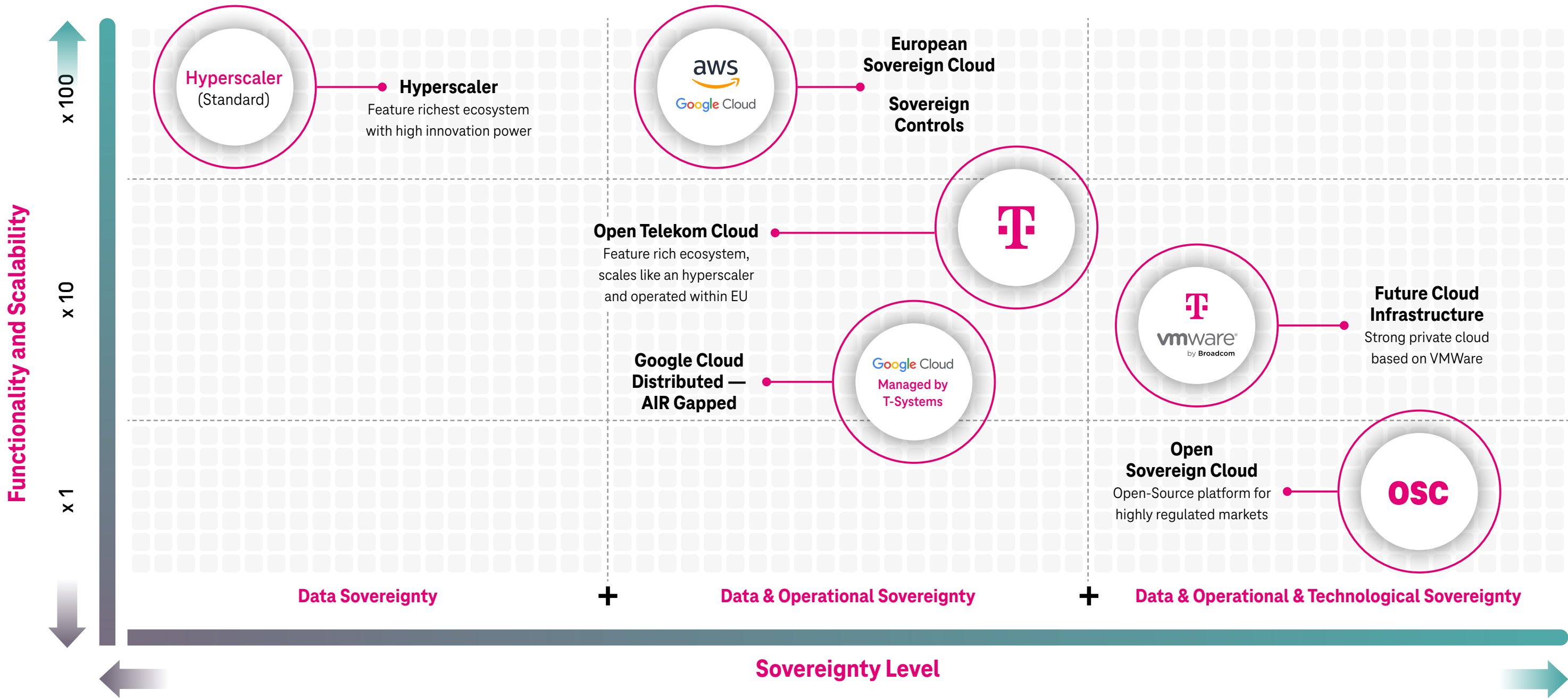
Open Sovereign Cloud (OSC) is based on open-source technology, enabling full digital sovereignty and preventing vendor lock-in. It is designed for highly regulated industries, guaranteeing maximum security, compliance, and flexibility in the cloud.

What are sovereign clouds? Here are the answers.

*expected to be available by the end of 2025

WHICH SOLUTIONS MEET MY REQUIREMENTS?

Find the right offering:



HOW OUR SOVEREIGN CLOUD PLATFORMS ENSURE SUCCESS

We have successfully guided customers from various industries on their journey to digital sovereignty in numerous projects



We are our best reference: Digital sovereignty at Deutsche Telekom

To accelerate its digitalization and drive innovation, Deutsche Telekom decided to embark on a multi-year transformation journey. A key goal is the consolidation and modernization of the group's SAP environment based on the cloud. For the project, which involves migrating several hundred ERP systems to the cloud, the group relies on the expertise of its subsidiary, T-Systems. The ERP systems have been moved to SAP S/4 HANA in T-Systems' private cloud (Future Cloud Infrastructure). T-Systems is responsible not only for the migration, consolidation, and management of the systems, but also for integrating and orchestrating hyperscaler resources into the multi-cloud environment as needed.

This approach achieves a balance: by migrating to a private cloud, Deutsche Telekom meets the GDPR requirements and the compliance mandates of the Federal Financial Supervisory Authority (BaFin). At the same time, key business areas such as logistics, procurement, and finance will operate more efficiently and flexibly, as new demands and innovations can be implemented more quickly in the public cloud.

[Learn more about the solution at Deutsche Telekom](#)



Healthcare: Digital identities at BARMER

In 2022, BARMER commissioned T-Systems and Verimi to provide and manage digital identities for its approximately 8.7 million insured members. Digital identities create trust online and are provided through ID services. T-Systems uses the Verimi ID Wallet, which is certified by the BSI, with the two partners having integrated the wallet into the BARMER app. To uniquely identify themselves, members store their electronic ID card and biometric methods like Face ID to produce personal identity data which can be conveniently used digitally—at the highest security level.

The digitalization of healthcare demands a particularly high level of protection, which also applies to projects within statutory health insurance companies. The data protection prevents insurers from processing their members' data unjustifiably; T-Systems hosts the solution in the Open Sovereign Cloud (OSC). This is suitable for organizations in regulated industries—Deutsche Telekom is committed to upholding social secrecy according to § 35 of the Social Code I (SGB I) throughout the group. The sovereign cloud solution covers the legal regulation by default and thus provides secure access to electronic patient records and prescriptions through smartphones, which in turn becomes the digital twin of the health insurance card. Digital identities can therefore serve as proof of insurance in the future. This project demonstrates how a sovereign cloud infrastructure can enable innovation while protecting sensitive health data.



[About the solution at BARMER](#)



University Hospital Schleswig-Holstein (UKSH): Full sovereignty over patient data

 **Benefits of digital
sovereignty for
the hospital:
Watch the video**

As the second-largest university hospital in Germany, UKSH has collaborated with T-Systems and Google Cloud to implement T-Systems' Sovereign Controls. This solution enables the secure digitalization of diagnostic results and serves as the foundation for AI applications in medical imaging, ensuring compliance with stringent German data protection laws. Encryption keys are exclusively managed in T-Systems' German data centers, guaranteeing full sovereignty over sensitive patient data.



Sovereign digitalization for the city of Kirchheim unter Teck

 **How the city uses the
BundesMessenger**

Kirchheim unter Teck is preparing for the future, with digital administration as a key tool. The large district town near Stuttgart aims to offer municipal services online and insists on sovereignty in the digital world to perform its tasks independently, autonomously, and securely. The city sought a messenger service for all employees that meets its security and sovereignty requirements.

T-Systems had the right solution with the Managed Service for BundesMessenger. Developed by BWI, the IT service provider of the German Armed Forces, it is available as open-source software. T-Systems operates the software in the sovereign German Open Telekom Cloud and provides it to public institutions as Software-as-a-Service. Updates and new releases are provided promptly as part of this managed service, and T-Systems also handles integration services.



Packaging manufacturer Gerresheimer: Maximum flexibility through multi-cloud

In recent years, Gerresheimer AG has acquired many companies, resulting in a heterogeneous IT structure that needed consolidation. By moving to the cloud, the provider of pharmaceutical packaging and medical accessories aims for more sustainability and efficiency. The company initially migrated systems to the Azure Cloud with Microsoft. Together with T-Systems, it then developed a multi-cloud strategy encompassing private and public clouds. However, it quickly became apparent that a complete migration of systems to the Azure Cloud was prohibited under privacy considerations. With T-Systems' sovereign Future Cloud Infrastructure (FCI), Gerresheimer achieves its primary goal of platform consolidation while increasing operational efficiency. The company now views its application landscape in a differentiated manner: systems requiring high innovation migrate to the Azure Cloud, where a unified landing zone from T-Systems offers state-of-the-art security. The remaining systems stay on T-Systems' Future Cloud Infrastructure.

 **Learn more about
the project**

KEY LEARNINGS: THE DOS AND DON'TS OF DIGITAL SOVEREIGNTY

Strategic measures companies should take and pitfalls they must avoid

HOW COMPANIES CAN BECOME MORE SOVEREIGN:



Reduce dependence on hyperscalers.

Open-source technologies support the independence and autonomy of companies and authorities



Strengthen autonomy.

Build internal expertise and have robust risk and crisis management which contributes to digital resilience



Protect the network.

Use tools such as next-generation firewalls, NIS2-compliant security policies, encryption, access controls, etc.



Work on future readiness.

Companies and authorities should familiarize themselves with modern technologies like AI

WHAT COMPANIES SHOULD AVOID:



Lack of diversification.

Tailored multi- and hybrid-cloud approaches provide solutions and reduce dependencies



Surrendering operational capability.

Even in cloud environments, companies and authorities must be able to customize their software and develop their own applications or services



Transferring control over business-critical processes.

Companies must be able to manage and control their cloud infrastructure themselves



Vendor lock-in.

Those wishing to change providers should be able to continue developing their solutions independently of them

Further information is available on our website:



[Click here for more information](#)

Do you have a question?

Feel free to contact us. Our consultants and expert teams will provide detailed answers to your questions about digital sovereignty and sovereign clouds.



[Go to the contact form](#)

Published by

T-Systems International GmbH
Marketing
Hahnstraße 43d
60528 Frankfurt am Main,
Germany

Sources:

¹European Cloud Provider, Synergy Research Group, 2022

²Studie Sovereign Cloud 2024, Foundry (formerly IDG Communications)