



MYRA

STATE OF DIGITAL SOVEREIGNTY 2025

Digital Sovereignty: Between Aspiration and Reality

Contents

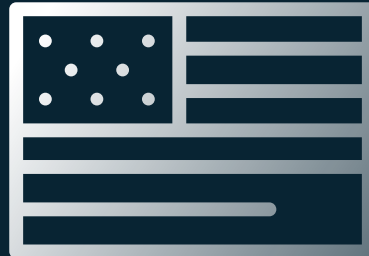
Executive Summary.....	3	From Dependency to Independence: Insights, Risks, and	
Digital Sovereignty: Between Aspiration and Reality	5	Recommendations for Action.....	12
Unity in Theory: Critical Infrastructure		The French Model: Promotion as a Decisive Stimulus.....	13
Needs a European Foundation.....	5	Specific Risks of Digital Dependency	13
Dependency: On the Digital Drip of Us Providers	6	Barriers to Switching and Strengths of European Providers	14
Visibility: Europe’s strengths are hardly known.....	8	Outlook: A Feasible Path to Greater Independence	14
Willingness to Change: Majority Sticks			
with US Solutions.....	9		

Executive Summary

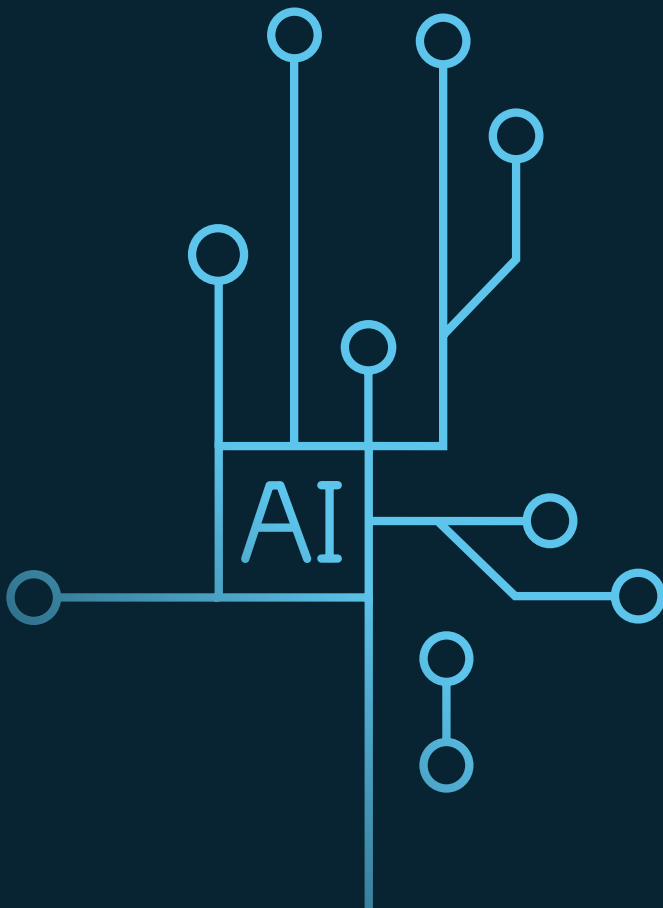
Digital sovereignty has been the focus of political strategies and expert discussions in Germany for years. However, a look at how it is actually implemented in corporate processes shows that there is still a striking difference between the stated goals and actual practice.

Although **84.4 percent** of IT decision-makers say that the government and critical infrastructure should primarily use European digital products, solutions from the US continue to dominate in their own companies. Only around a third of companies plan to introduce European software in the next 24 months. Almost half rule out a switch at present.

Meanwhile, a significant proportion of companies see strong dependencies on non-European providers in key areas such as cloud services and IT security (around **40 percent** in each case). European solutions have played a minor role to date: less than **25 percent** of companies use European cloud services. In the area of collaboration tools or AI infrastructure, the figure is around **10 percent**. In addition to a lack of willingness to implement, there is often a lack of information about European alternatives. Especially in innovation-driven fields such as AI or cybersecurity, many IT managers are not sufficiently informed about European counterparts. The result is a continuing preference for US solutions despite alternative offerings.



Despite the fact that European software solutions are not widely used in many areas and are often little known, IT decision-makers frequently underestimate their own dependence on non-European providers. Only **21.9 percent** say they are familiar with European AI solutions, and only **10.2 percent** use them. Nevertheless, more than half (**50.3 percent**) rate their dependence in this area as low or non-existent. The picture is similar in cybersecurity. Only one in three is aware of European offerings. Only **20.5 percent** use them. However, almost half (**47.2 percent**) see only a weak to non-existent dependence.



The bottom line is that German companies remain heavily dependent on US IT providers – but not in all areas. In traditional domains such as ERP, finance, and HR software, European providers hold market shares of **30 to 40 percent**.

German IT decision-makers are generally open to switching to European alternatives – under clear conditions. Two-thirds of companies would switch to European providers if performance and security were comparable. Data storage is particularly important here: for **62.5 percent** of those surveyed, guaranteed data storage in the EU is a decisive criterion for the future use of European software.



Symbolic tech patriotism is not enough

To really kick off a lasting shift toward digital sovereignty, we need more than just symbolic commitments. This means that manufacturers need to bring convincing products to market, and politicians need to support a change of course by creating favorable conditions and offering incentive programs. They can also draw public attention to domestic tech companies by showcasing flagship projects. Until price, performance, and political will come together, digital independence will remain a pipe dream.

Digital Sovereignty: Between Aspiration and Reality

Digital sovereignty is considered a key prerequisite for long-term competitiveness in politics and business. However, until now there has been a lack of reliable data on the extent to which German companies actually depend on non-European providers in key technology areas, in which fields European alternatives are already being used, and which factors could encourage a switch.

This study closes this gap.

Based on a representative Civey survey of 1,500 IT decision-makers, it assesses the current state of digital sovereignty in Germany in eight areas, including cloud services, cybersecurity, and AI infrastructure.

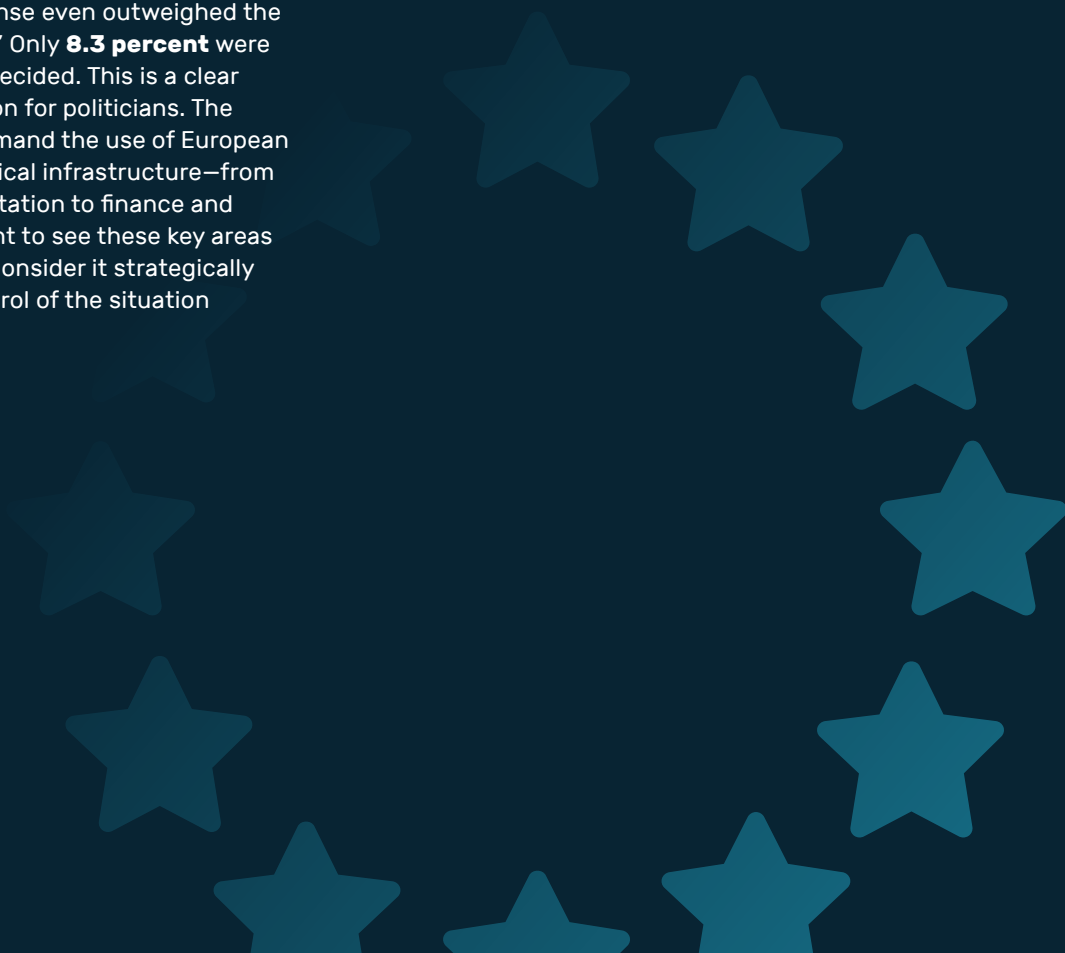
The report highlights the areas where viable European options already exist, where there is still room for improvement, and the levers that politics and business can use to promote digital independence.

The study thus provides a solid basis for informing the debate on digital sovereignty with concrete data and recommendations for action.

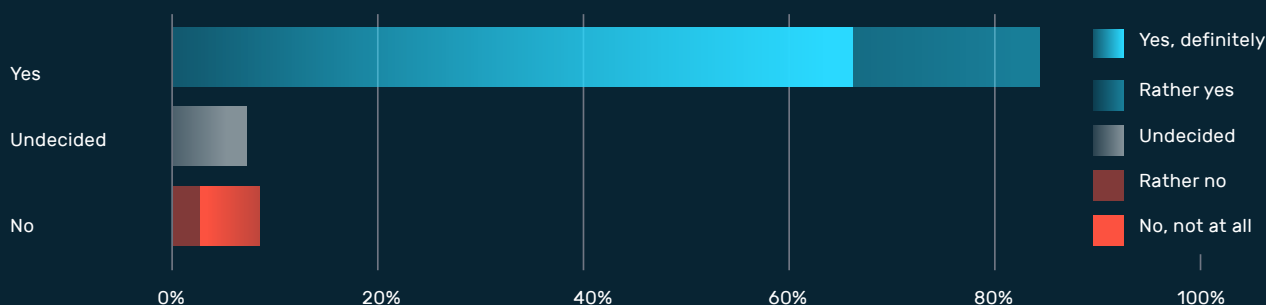
Unity in Theory: Critical Infrastructure Needs a European Foundation

When asked whether countries and operators of critical infrastructure should use European providers in order to remain independent of non-European providers, IT managers gave a very clear answer:

84.4 percent said yes. It is noteworthy that the clear “yes, definitely” response even outweighed the more moderate “rather yes.” Only **8.3 percent** were against it, with the rest undecided. This is a clear vote and a clear call to action for politicians. The message is that experts demand the use of European solutions, especially for critical infrastructure—from energy, water, and transportation to finance and healthcare. They do not want to see these key areas in non-European hands or consider it strategically dangerous not to be in control of the situation themselves.



In your opinion, should countries and operators of critical infrastructure in Europe use European providers for digital products in order to be independent of non-European providers?



IT decision-makers agree: the public sector and operators of critical infrastructure should rely on European solutions.

The mood among the companies surveyed is in line with political trends: The European Union and the German government are pushing for stricter regulation of cloud and communication services for critical infrastructures, as demonstrated by the NIS 2 Directive and national legislative initiatives. Measures such as the planned exclusion of certain providers from security-critical

networks make it clear that in future, “trustworthy” providers will be given preference. The business community has signaled its general approval of this, especially when it comes to the public sector and critical infrastructure. However, companies are much more hesitant when it comes to their own IT infrastructure.

Dependency: On the Digital Drip of Us Providers

Dependence on non-European solutions in various areas

Summary of results

Area	Strong	Undecided	Low / Not at all
ERP	19.8%	12.0%	68.2%
CRM	25.0%	12.6%	62.4%
Cloud Service	39.7%	12.7%	47.6%
Collaboration	36.6%	12.6%	50.8%
Cybersecurity	39.5%	13.3%	47.2%
Finance	16.8%	12.0%	71.2%
HR	13.5%	10.4%	76.1%
AI infrastructure	36.6%	13.1%	50.3%

The analysis shows that German companies continue to rely heavily on non-European providers in security-related technology areas. **39.7 percent** of IT decision-makers report strong to very strong dependence in the area of cloud services. In the area of cybersecurity, **39.5 percent** give a similar assessment. Four out of ten companies feel that they would be unable to operate in these critical areas without non-European technology. AI infrastructure is also rated as highly dependent on non-European solutions by **36.6 percent**.

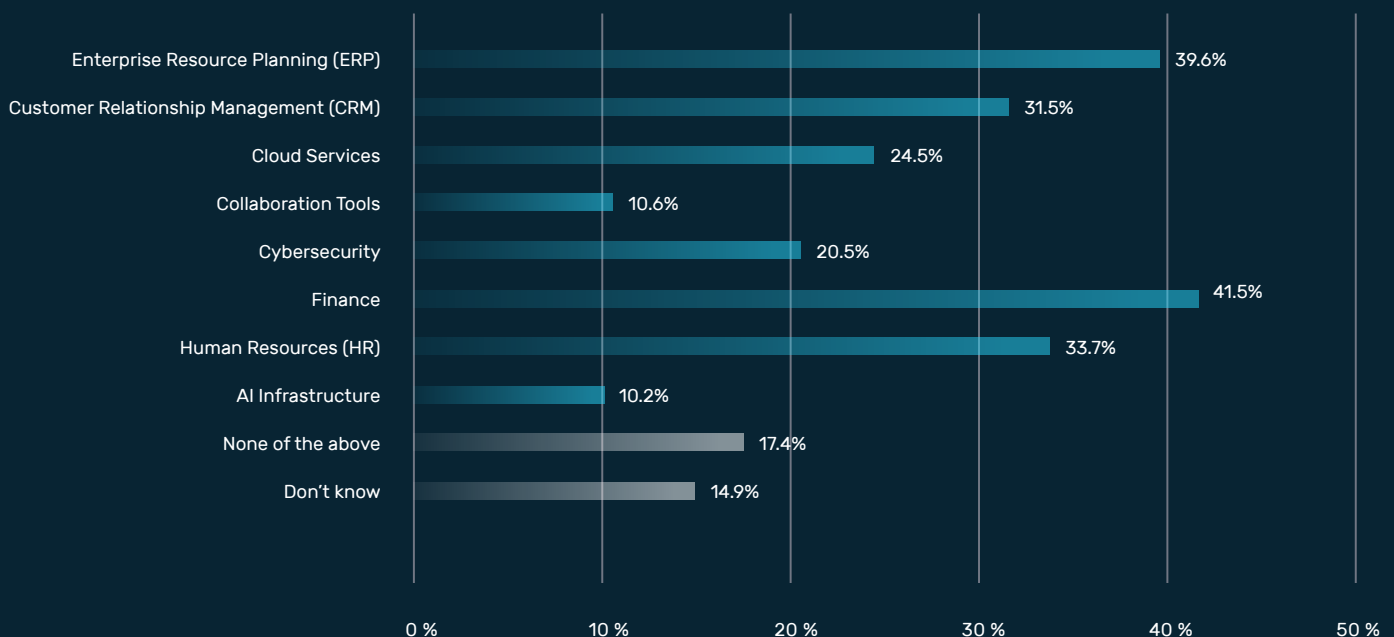
In contrast, there is less dependence in individual segments such as financial software (**16.8 percent**) and ERP systems (**19.8 percent**), as European providers traditionally play a stronger role here. However, these areas of relative independence cannot hide the fact that non-EU providers are still predominantly relied upon in key areas such as cloud, AI, security, and collaboration—precisely where sensitive data is processed and forward-looking decisions are made.

Companies Misjudge Their IT Sovereignty

Although European software is rarely used in many areas, IT decision-makers generally rate their level of dependency as very low. This means that the degree of dependency is greatly underestimated and the degree of independence massively overestimated. Although only **10.2 percent** use European AI infrastructures, more than half of those surveyed (**50.3 percent**) rate their dependence on non-European solutions in this area as low to non-existent. The picture is similar in cybersecurity. Only **20.5 percent** use European security solutions. However, almost half (**47.2 percent**) see only a weak to non-existent dependency.

20,5%
use European
cybersecurity

Which of these business areas does your company already use European software solutions for?



When it comes to the use of European software products, there are significant differences between categories.

In areas where European providers traditionally have a stronger presence, such as ERP and financial software, subjective perceptions and actual usage are more closely aligned. For example, **68.2 percent** of respondents feel that they have little to no dependence on ERP systems and **71.2 percent** feel the same about financial software, which is supported by the comparatively high use of European solutions (**39.6 percent** for ERP and **41.5 percent** for financial software).

Visibility: Europe's strengths are hardly known

A significant proportion of IT decision-makers are unfamiliar with European software alternatives. When asked in which areas they are familiar with European software solutions, slightly more than one in ten IT managers say they are not familiar with any; a further **16 percent** answer "don't know." This means that a considerable proportion of those responsible lack an overview of available European products in key categories of enterprise software. The lack of awareness of European solutions is a serious obstacle to digital sovereignty.

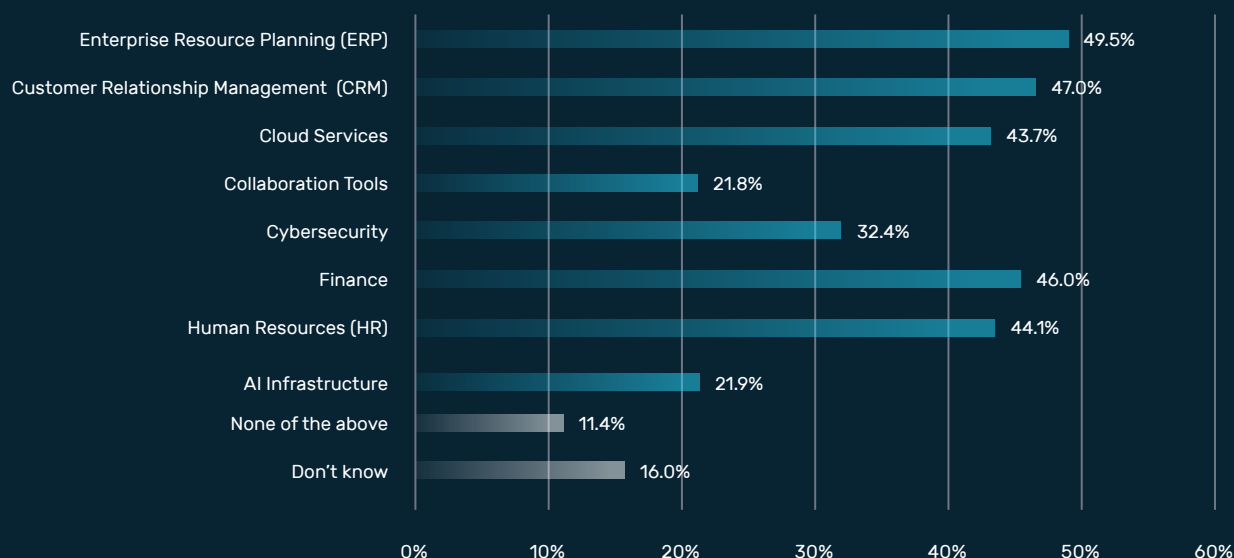
A detailed look at individual software areas reveals a clear gap in awareness of European providers. European solutions are relatively well represented in

traditional segments such as ERP, CRM, and financial software: **49.5 percent** of respondents are familiar with European ERP providers, **47.0 percent** can name companies in the CRM sector, and **46.0 percent** in finance. This strong presence is no coincidence, but rather reflects the long tradition of European – especially German – software companies in these fields.

In contrast, awareness of European alternatives in newer technology areas is significantly lower. Only **21.8 percent** of IT decision-makers are familiar with European solutions for collaboration tools, even though these have become much more important during the pandemic. US providers continue to dominate here, while European or open source solutions are only known to a small circle. The picture is similar for AI infrastructure: only **21.9 percent** can name a European provider, which underscores Europe's low visibility in this future-oriented field dominated by US corporations.

In the area of cybersecurity, awareness of European providers still has room for improvement: only **32.4 percent** of IT managers are aware of European alternatives. This shows that although some European companies have already established themselves, there is still a considerable need for information and development. The situation is somewhat more positive in the cloud segment: **43.7 percent** of respondents are familiar with a European cloud service – a relatively high figure compared to other technology fields.

For which of these business areas are you familiar with European software solutions?



Awareness of European software providers by application area (percentage of IT decision-makers who are familiar with European solutions)

The evaluation suggests that European software is particularly popular in areas where it has been established for a long time. In newer digital fields of application, however, European solutions are not very widespread. In the area of IT security, **20.5 percent** of companies rely on European products, which underscores the importance of specialized European providers. However, the majority continue to rely on comprehensive solutions from the US. It is striking that only **17.4 percent** of respondents say they do not use European software in any area – more than **80 percent** use at least one European solution. Nevertheless, non-European products continue to dominate the market.

80%

use at least
one European
solution

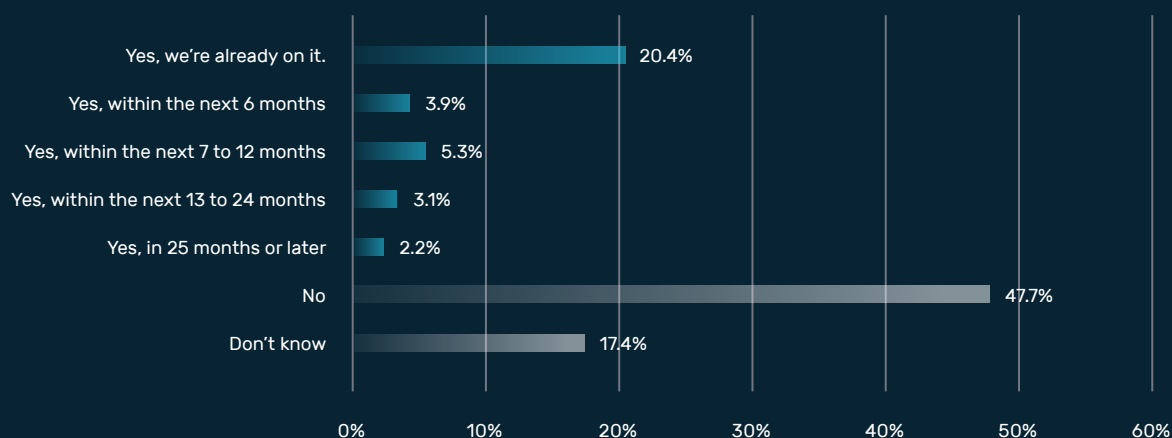
Willingness to Change: Majority Sticks with US Solutions

Despite that, companies are calling for the consistent use of European software solutions in the public sector and for critical infrastructures, they are themselves much more cautious when it comes to planning the introduction of European software solutions in the future.

Only **20.4 percent** of the companies surveyed are already actively introducing one or more European solutions. Another **15 percent** plan to do so within the next two years (**3.9 percent** in the next 6 months, **5.3 percent** in 7 to 12 months, **3.1 percent** in 13 to 24 months, **2.2 percent** in 25 months or later). On the other hand, over **47 percent** say no, they have no such plans. Just under a fifth are undecided or don't know (**17.4 percent**). Overall, the majority of companies are sticking with tried-and-tested solutions for the time being; there is no clear trend toward greater digital sovereignty as yet.



Is your company planning to introduce one or more European software solutions in the future?



Almost half of all IT decision-makers do not plan to introduce European software products within the next two years.

What prevents the majority from taking action?

A key reason for the hesitance of many companies lies in the challenges and risks associated with IT migrations. Such changes are complex and often affect core business processes. Changes are therefore only made when they are absolutely necessary or required by law. Companies act primarily on the basis of facts and within the framework of legal requirements. Without significant added value or regulatory pressure, the motto “Never change a running system” applies.

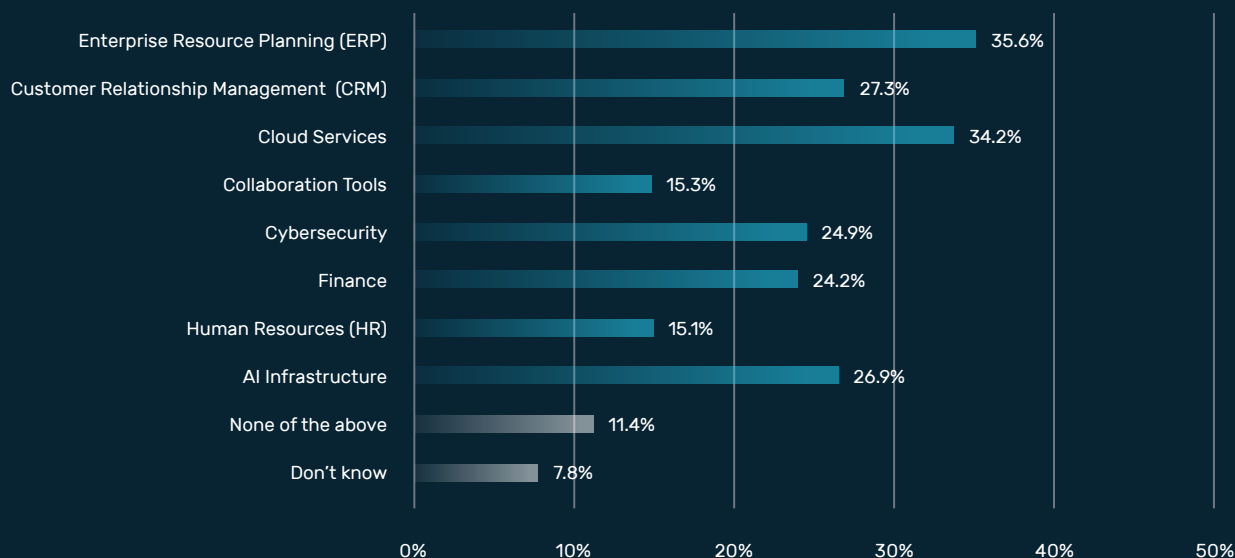
The analysis of switching intentions shows that companies with plans to switch are primarily looking to take action in the areas of ERP (**35.6 percent**) and cloud services (**34.2 percent**). AI infrastructure (**26.9 percent**), CRM (**27.3 percent**), and financial software (**24.2 percent**) are also in focus. In the cloud sector in particular, which was previously identified as an area of dependency, some companies have concrete plans to establish European alternatives. The figures also indicate that European providers in the finance and CRM sectors could further expand their already strong market position.

In contrast, the proportion in the collaboration tools segment is low: only **15.3 percent** want to make changes in this highly dependent category over the next 24 months.



Which of these business areas does your company plan to introduce a European software solution in over the next 24 months, or is already in the process of doing so?

IT decision-makers whose companies plan to introduce a European software solution within the next 24 months



Areas in which IT decision-makers are planning to introduce European software solutions.

Turning Your Back on Big Tech? Yes, But ...

German companies are generally very willing to switch from established, mostly US-based IT solutions to European alternatives – provided that the objective criteria are right. Performance parity is the most important decision-making criterion: **69.9 percent** of IT decision-makers would switch to European software if it offered the same functionality and reliability as their existing solution. Data security is almost as important: **69.4 percent** cite it as their main reason for switching. Cost advantages also play a key role; two-thirds (**66.5 percent**) of companies would be willing to switch to European solutions if the costs were significantly lower. More than half (**57.4 percent**) also see subsidy programs as a helpful incentive.

These results show that there is openness to European alternatives, provided that they can compete with established solutions on key points. In addition to hard facts such as performance, safety, and costs, supporting measures – such as subsidy programs or regulatory frameworks – are also important factors in persuading companies to switch.



Willingness to switch based on various criteria





















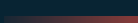
Summarized results

Area	Yes	No	Don't know
Cost factors	66.5%	22.3%	11.2%
Similar services	69.9%	20.4%	9.7%
Subsidies	57.4%	29.8%	12.8%
Data security	69.4%	20.9%	9.7%
Acknowledgment	48.4%	37.3%	14.3%
Prohibition	57.8%	29.5%	12.7%

The main criteria for switching are performance, data security, and costs.

Willingness to use European solutions in the future based on various criteria

Summarized results

Criteria	High	Undecided	Low
GDPR compliance	59.4% 	14.5% 	26.1% 
Data storage in the EU	62.5% 	13.1% 	24.4% 
Local support	61.3% 	13.7% 	25.0% 
Strengthening euro economy	45.3% 	22.8% 	31.9% 
EU-basierte Datenübertragung	51.9% 	20.6% 	27.5% 
EU-based data transfer	53.0% 	22.3% 	24.7% 
CDN	37.0% 	29.5% 	33.5% 

European data protection standards and local support are the most important criteria for many decision-makers when considering the future use of European solutions.

62.5 percent of respondents say they would be very willing to use European software solutions in the future if data storage in the EU were guaranteed. A similarly high proportion (**61.3 percent**) consider local support to be a decisive factor. Strict compliance with the GDPR also convinces **59.4 percent** of IT decision-makers. These results illustrate that the core promises of European providers – a higher level of data protection and customer proximity – are key selling points. In addition, idealistic aspects also play a role: for **45.3 percent** of respondents, strengthening the European economy is an important motivation, although this motive weighs less heavily than the concrete, practical advantages.

From Dependency to Independence: Insights, Risks, and Recommendations for Action

In Germany, there is a significant gap between the desire for digital sovereignty and the reality in companies and public authorities. The actual dependence on non-European, mostly US technology providers is high and its consequences are massively underestimated.

At the same time, the political mandate for action is clear: a broad consensus of **84 percent** of IT decision-makers demands that the public sector and critical infrastructures give preference to European IT solutions. If the state sets a good example here, this could trigger a wave of change, as the fundamental willingness is already there in the business community.

The French Model: Promotion as a Decisive Stimulus

With its “**Parcours de cybersécurité**” program launched in 2021, France is demonstrating how government funding can effectively strengthen digital sovereignty.

- **Framework:** Under the leadership of the national cybersecurity authority ANSSI, a total of **945 institutions** – including municipalities, hospitals, and other public institutions – were supported with a budget of €176 million.
- **Implementation:** The program included standardized audits and co-financed implementation of over 3,000 specific security measures such as system hardening, network segmentation, and backup strategies.
- **Result:** The average cyber maturity level of participants rose significantly from “D+” to “B.” In addition, municipalities invested an average of **30 percent** more than was provided for in the funding, demonstrating a strong commitment.

Experience in France and survey data confirm that financial incentives are a key lever. More than half of decision-makers would consider switching to European providers if appropriate subsidies were available. Once the financial hurdles in France were removed, the majority of participants preferred European service providers. A “sovereignty check” for public IT procurement introduced in Germany could legally anchor the examination of European alternatives and increase their visibility.

Specific Risks of Digital Dependency

The technological dependencies of European companies on non-European suppliers pose concrete risks with immediate consequences:

- **Loss of control:** A clear example of this is Microsoft’s blocking of the email account of the chief prosecutor of the International Criminal Court in May 2025. This measure, apparently triggered by US political sanctions, led to a temporary failure of important communication channels and highlights the danger of unilateral dependence on US providers.
- **Economic pressure:** Rising license costs can place a significant burden on companies and public institutions. The city of Copenhagen, for example, was faced with a **72 percent** price increase for Microsoft products between 2018 and 2023, prompting it to switch to open source alternatives such as LibreOffice. Similar developments can also be observed in other European cities such as Lyon, which are increasingly turning to open and European solutions to control costs and strengthen their own digital sovereignty.
- **Legal uncertainty:** US laws such as the CLOUD Act and Section 702 of the Foreign Intelligence Surveillance Act (FISA) require US providers to hand over data to US authorities – regardless of whether the data is stored on European servers. This undermines the European General Data Protection Regulation (GDPR), deprives companies of control over their data and jeopardizes their competitiveness.

These examples illustrate that dependence on non-European technology providers not only poses theoretical risks, but also has real and immediate consequences for the digital sovereignty, economic efficiency, and legal certainty of European companies and institutions. Strengthening our own digital infrastructures and using European solutions are therefore key steps toward minimizing these risks.



Barriers to Switching and Strengths of European Providers

Despite the known risks, almost half of IT decision-makers (**47 percent**) do not intend to make any changes to their existing IT infrastructure in the next two years. A major reason for this is a lack of knowledge about high-performance European alternatives – a circumstance that further consolidates the strong market position of non-European providers.

However, European solutions have clear unique selling points that also offer economic advantages:

- **Legal certainty** through compliance with EU law and GDPR
- **Data protection** without access for foreign authorities
- **Local service** with short distances and on-site contact persons

However, these advantages alone are not enough. In order to remain competitive in the long term, European providers must offer convincing performance and prices, as these factors continue to be decisive for companies.

Outlook: A Feasible Path to Greater Independence

Awareness of the need for digital sovereignty is greater than ever. The goal is not technological isolation, but rather the creation of a resilient, innovative, and competitive digital ecosystem based on European values and legal certainty.

If policymakers now create bold and reliable framework conditions and companies actively embrace change, Europe can gradually regain its digital independence. Continuing with business as usual would reduce digital sovereignty to mere lip service, while the risks of dependency continue to grow.



Figures, Data, Facts: Our Reports on Cybersecurity and Digital Sovereignty

Would you like to learn more about cyber resilience and digital sovereignty in Germany? Our comprehensive studies provide you with the latest figures, exclusive data, and expert insights into Germany's most pressing digital challenges.

Myra Cybersecurity Report H1 2025

How has the threat landscape evolved? Which industries are particularly at risk, and what types of attacks should companies expect? Discover the facts behind the headlines. Find all the details in our Cybersecurity Report:



Myra State of Digital Sovereignty 2025

(Digital version of the study + additional material)

Where does Germany stand in the global competition for technological independence? Find out why digital sovereignty is a crucial strategic factor for the economy and society and what challenges need to be tackled. For the complete analysis:



Methodological note: The results are based on a Civey survey of 1,500 IT decision-makers in Germany between April 2 and June 10, 2025. The survey was conducted online; multiple answers were possible for questions with multiple options. The statistical margin of error is approximately ± 5 percent. Digital sovereignty is defined here as the ability to use European software solutions instead of being dependent on non-European providers.

Made in Germany



We Protect What Matters. In the Digital World.

Want to learn more about how our solutions can increase your revenue, minimize your costs, and protect your applications from malicious attacks?

Our team of experts is ready to help you develop a customized solution for your business.

Schedule a no-obligation consultation today!

**Cyber attacks are expensive,
a non-binding conversation costs nothing.**

Myra Security GmbH

☎ +49 89 414141 - 345
🌐 www.myrasecurity.com
@ info@myrasecurity.com