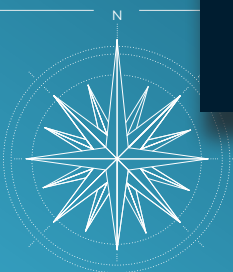
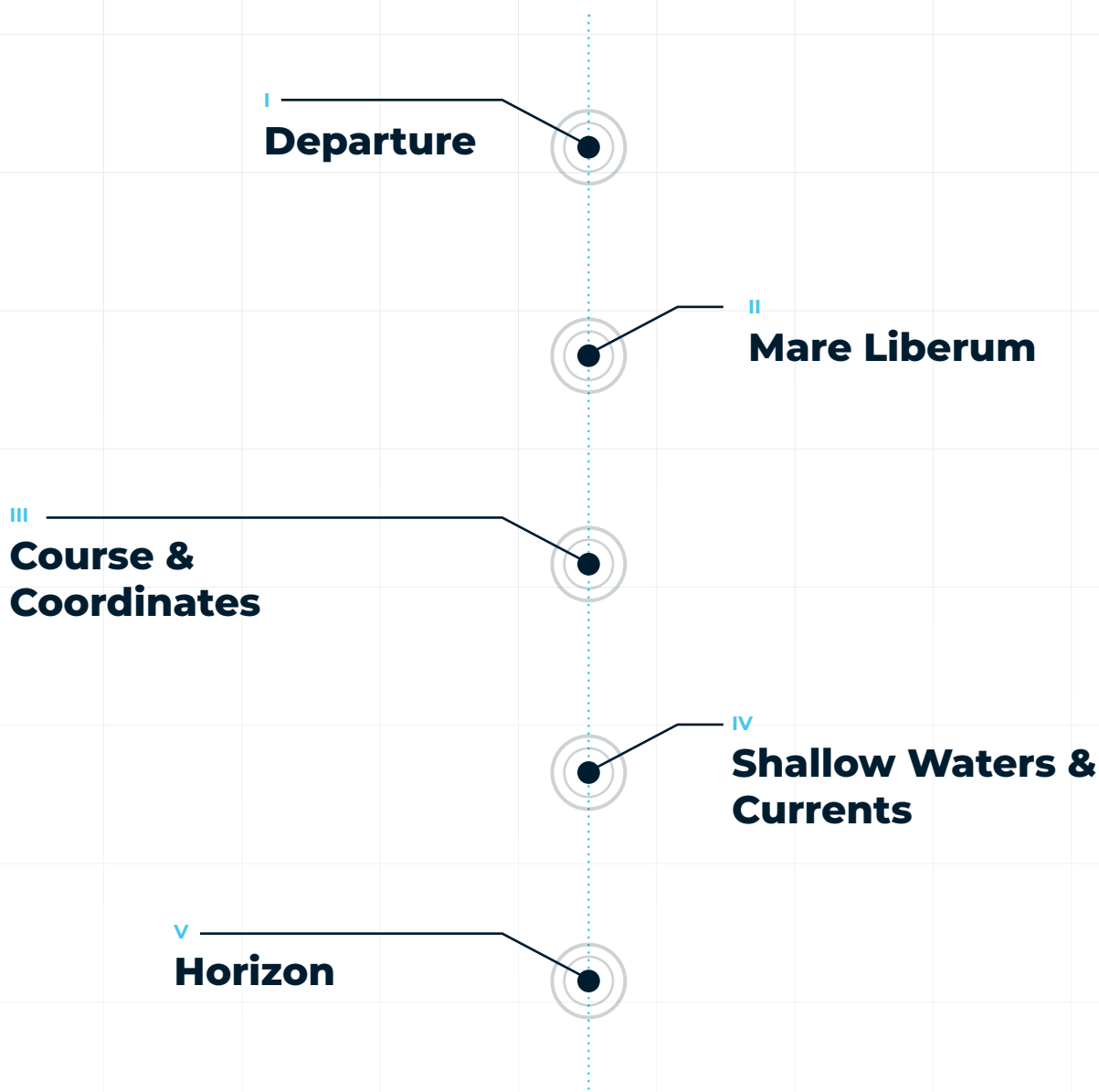




STATE OF DIGITAL SOVEREIGNTY 2026

Uncharted Waters





Contents

I Departure	3	IV Shallow Waters & Currents	17
About this study.....	4	Europe's New Trade Routes: Where Sovereignty Is Most Urgent	18
Foreword: Taking the wheel.....	5	The challenges to migration: Why it's hard to change the course.....	20
Executive Summary: Key Findings at a Glance	7	The CLOUD Act as a warning sign: Between waiting and taking action.....	22
II Mare Liberum	9	V Horizon	25
Mare Liberum: From the Free Sea to the Free Web.....	10	A View of the Horizon: How realistic is digital independence by 2035?.....	26
III Course & Coordinates	11	Conclusion: Europe does not need to own the digital ocean. But it has to be able to navigate on its own again.	28
Germany: A Year-Over-Year Comparison, 2025/2026: From Commitment to Action	12		
Three regions, one mission: Germany, France and the Nordic countries	14		



New Beginning



About this study

Digital sovereignty has long since ceased to be a marginal political issue in Europe. It is at the center of strategic debates – in government ministries, boardrooms, and data centers. Yet there still seems to be a considerable gap between the aspiration for independence and reality.

Last year's edition of the State of Digital Sovereignty Report was therefore published with a clear mission: to provide robust data to support a debate that, until then, had consisted primarily of political statements and strategy papers. The result was clear – the desire for sovereignty was strong, but implementation lagged behind. Theory had not yet been put into practice. And there was a glaring gap between subjective perception and reality.

In just one year, the context of debates on sovereignty has changed significantly. Geopolitical tensions have shifted IT strategies, the CLOUD Act has moved higher on the agenda, and media reports about diplomats who are said to be actively lobbying against sovereignty laws make it clear: Digital independence has evolved from a matter of technical implementation to a matter of political agency.

It seems that in 2026, Europe will be sailing into waters that are, in part, uncharted. This year's report, "State of Digital Sovereignty: Accordingly, Uncharted

Waters" examines not only what has changed since last year, but also the course that key European players are taking.

The report broadens its scope beyond Germany to include IT decision-makers in France and the Nordic countries of Denmark, Sweden, Norway, and Finland. Germany, France, and the Nordic countries: Three regions that shape Europe – and each of which conceives, prioritizes, and implements digital sovereignty in its own way.

"Uncharted Waters" is not intended as a report on shortcomings, but rather as a map for setting out on a new journey – with coordinates that show how far Europe has already come, where the shallow waters are, and which routes lead forward.

Foreword:

Taking the wheel



48° 08' 24.2" N
11° 31' 19.8" E

Europe stands on the bridge of a ship that has long been navigated using foreign maps. The routes were familiar, the ports were safe, and the instruments were reliable. But suddenly, the horizon shifts. Trade routes that seemed safe just yesterday are now navigating political shoals. Technology, which once promised above all efficiency, now determines our freedom of action.

Digital sovereignty often sounds like a defensive stance or a retreat from the collective path. The opposite is true. Sovereignty does not mean shutting the world out. It means being able to chart your own course. Those who act with confidence can choose their partners, better assess risks, set standards, and limit dependencies. Anyone who can't do that will eventually find out that they aren't the captain after all, but just a passenger – even if they're paying for the cargo.

"Sovereignty does not mean shutting the world out. It means being able to chart your own course."

Myra Security is named after Nicholas of Myra – a saint who is still regarded today as the patron saint of sailors and merchants and is thus deeply rooted in Germany's Hanseatic cities. This historical thread fits our present day with astonishing precision. In the past, merchants and captains had to know which winds they could rely on, which routes were safe, and which ports offered shelter. Today, companies and government agencies need to know which infrastructures they can trust with their data, processes, and business models – and which ones they cannot. Even in the debate over sovereignty, the "Netz" bears strong parallels to the history of seafaring. In 1609, the Dutch jurist Hugo Grotius wrote in *Mare Liberum* that the sea could not belong to anyone and must be open to all nations. In doing so, he challenged a power-based order in which Spain and Portugal

laid claim to trade routes, seas, and access points as if oceans could be fenced off like farmland. Grotius, one of the founding fathers of the concept of sovereignty as set forth in, disagreed. He articulated an idea that would later shape global trade: Open spaces need fair rules. Otherwise, they become instruments of power.

Today, the most important economic routes no longer run across oceans, but through data centers, cloud platforms, software stacks, and security services. Whoever controls this infrastructure does not control everything – but enough to put pressure on markets, governments, and companies. That is precisely why the debate and the importance of sovereignty are gaining renewed significance.

The results of this study show: Europe wants to change course and is already doing so. IT decision-makers in Germany, France, and the Nordic countries view digital sovereignty as a strategic priority. What still read more like a statement of intent in 2025 is turning into a movement in 2026.

Of course, the waters ahead of Europe are far from calm. However, Europe does not need to own the digital ocean. It must be able to navigate on its own again.

Over the years, many companies and institutions have built up software landscapes that have grown like fleets: Plank by plank, deck by deck, with deeply ingrained routines and crews who have been operating the same instruments for decades. No one can retrofit fleets like these overnight. However, there is a broad consensus that they must adapt in light of changing times – this study provides a roadmap for this process.



Katharina M. Schwarz
Head of Global Communications
Myra Security GmbH



**Europe does not need
to own the digital ocean.
It must be able
to navigate on
its own again.**

Executive Summary

Digital sovereignty has taken hold in European companies – no longer just a political buzz, but a strategic guiding principle.

The results of this study, which surveyed IT decision-makers in Germany, France, and the Nordic countries, paint a clear picture: The drive toward digital independence is growing, and it is increasingly reflected in concrete decisions.

The desire for sovereignty is maturing – and gaining broader support

In Germany, 87.5 percent of IT decision-makers support the preferential use of European digital products in critical infrastructure – up from 84.4 percent the previous year. Support is growing, but it is distributed differently: The percentage of respondents who answered a clear “Yes, definitely” fell from 66.1 to 47.2 percent, while the percentage who answered “Somewhat yes” rose from 18.3 to 40.3 percent. That conviction remains – but it becomes more grounded, more mature, and more measured. What is noteworthy here is the almost complete disappearance of clear rejection: Only 0.3 percent now say that European products in the critical infrastructure (KRITIS) sector should not be given preference under any circumstances, compared with 5.5 percent last year. In a comparison of countries, France leads with a combined approval rating of 93.6 percent, followed by the Nordic countries with 88.9 percent, and Germany with 87.5 percent.

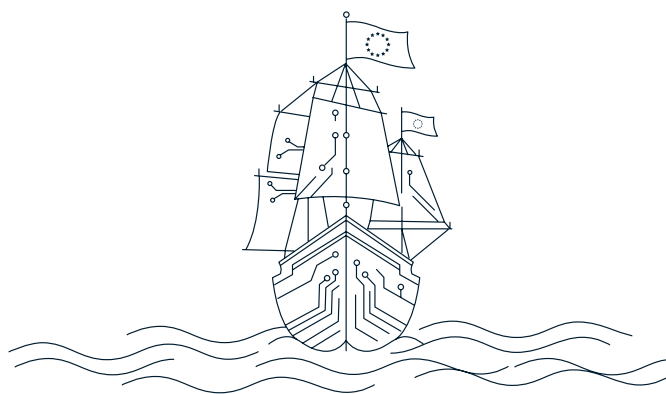
From desire to action – a turnaround in numbers

Within a year, digital sovereignty is shifting from a matter of attitude to a matter of implementation. In 2026, nearly twice as many companies in Germany will be actively implementing European software solutions: 39.7 percent, compared with 20.4 percent the previous year. The percentage of those planning to switch within the next six months has risen by more than 400 percent, from 3.9 percent to 20.4 percent. At the same time, the percentage of decision-makers who do not want to implement European software has plummeted almost entirely, from 47.7 to 4.6 percent. The number of undecided voters has dropped from 17.4 to 3.9 percent. A clear about-face. A comparison with other European countries also shows that in all three regions, only a negligible minority fundamentally rejects European software – 4.6 percent in Germany, 3.3 percent in the Nordic countries, and 2.4 percent in France.

Three regions, three personalities

A comparison across Europe reveals different mentalities. France leads the way with 93.6 percent, driven by a fundamental commitment to prioritizing European software in the public and KRITIS sectors. At the same time, in response to geopolitical events, France is relying even more heavily on U.S. software.

24.8 percent of French IT decision-makers report this, compared with 19.8 percent in Germany and 16.9 percent in the Nordic countries. However, political decisions made after the survey period – including the French government’s announced migration to Linux – suggest that a shift in policy is beginning. The Nordic countries stand out for their consistency and steadfastness: Across all planning horizons, their approval ratings remain consistently high, and only 3.3 percent categorically reject a change. Germany presents the most balanced picture: a high willingness to take action, a pragmatic assessment of risk, and the highest switch rate as a result of the CLOUD Act.



Geopolitics as a catalyst – but not a clear-cut one

Recent events have changed IT strategies in all three regions. About half of all respondents say they have placed greater emphasis on their own sovereignty – 51.5 percent in Germany, 50.0 percent in France, and 48.9 percent in the Nordic countries. In terms of the use of European software, the Nordic countries lead with 50.8 percent, followed by Germany with 47.8 percent and France with 40.3 percent. The fact that, at the same time, a significant proportion of users in all regions relies more heavily on U.S. software shows that geopolitical uncertainty acts as a catalyst, but it does not steer in the same direction.

Obstacles remain but the majority sees opportunities

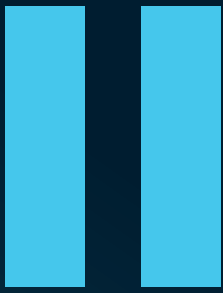
Across all regions, IT decision-makers consider high migration costs, a lack of information about European alternatives, and technical concerns as the biggest barriers to switching. But the key perspective is the reversal: If slightly more than two-thirds of German IT decision-makers do not cite high migration costs as a major obstacle, the overall picture is less a map of obstacles than a map of available potential. France shows the most optimistic outlook: 7.1 percent see no obstacles at all – compared with 5.9 percent in the Nordic countries and 5.7 percent in Germany. The biggest challenge, then, is not to overcome resistance, but to provide direction.

Europe believes in its digital transformation – the North is leading the way

Across all regions, cybersecurity, artificial intelligence, and cloud services are emerging as the technology sectors most critical to sovereignty. The CLOUD Act is no longer just a legal technicality: In none of the three regions does the percentage of respondents who are unfamiliar with it exceed 4.0 percent. And the outlook for the future is surprisingly optimistic – though there is a striking regional disparity: 49.5 percent of Nordic IT decision-makers believe that Europe achieving a high degree of digital independence within the next ten years is realistic, compared to 39.6 percent in Germany and 33.7 percent in France. What is particularly revealing here is the nature of this confidence: While 68.4 percent of European companies in the Nordic countries say they are capable of developing digitally competitive products in most areas, the figure is 50.6 percent in France and only 45.8 percent in Germany. The North doesn't just believe that Europe can do it – it believes that Europe can already do it.

49,5 %

of Nordic IT decision-makers believe that Europe achieving a high degree of digital independence within the next ten years is realistic



Mare Liberum

Mare Liberum – from the free sea to the free web

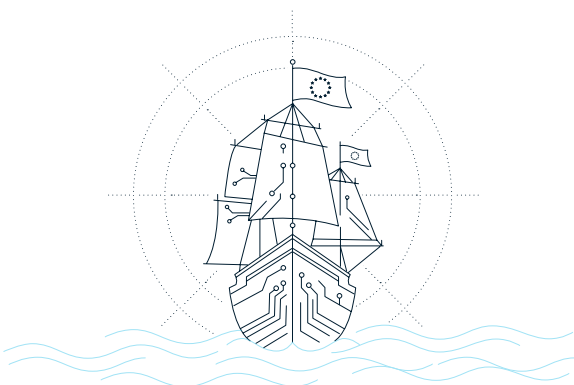
Hugo Grotius, the Santa Catarina, and an idea that changed the world

In 1603, ships of the Dutch East India Company captured the Portuguese merchant ship Santa Catarina in the Strait of Malacca off the coast of Singapore. It wasn't an ordinary robbery. It was a political act – in the midst of a power struggle over trade routes, spices, and control of the world's oceans.

Spain and Portugal had divided the world among themselves. The Treaty of Tordesillas (1494) drew a line across the Atlantic with Spain to the west and Portugal to the east. The seas, it was claimed, belonged to these crowns. The Netherlands saw things differently – and commissioned a young lawyer to draft this objection: Hugo Grotius.

In 1609, his work *Mare Liberum* – The Free Sea was published. Grotius argued: The sea can not belong to anyone. By its very nature, it is open to all nations. Whoever lays claim to it – is laying claim to the unclaimable.

For some, it was a theory detached from reality while for others, it was a legal weapon in an economic tug-of-war. In any case, however, it marked the beginning of a line of thought that continues to shape international law to this day: shared spaces need fair rules – otherwise, they will become instruments of power for the few.



Every generation has its own seas

Grotius's concept of the high seas prevailed. It became the foundation of modern global trade and, in its most profound sense, of the very concept of sovereignty itself.

Today, the world economy's most important trade routes no longer cross oceans. They run through data centers, cloud platforms, software stacks, and security services. Today, spice ships are called data streams. Seaports are now called hyperscalers. The new bottlenecks are APIs, license agreements, and encryption standards.

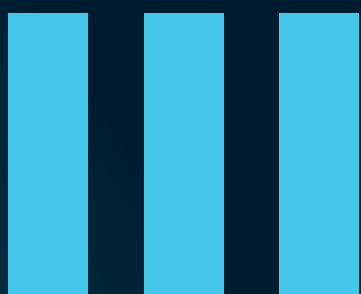
Once again, a handful of players are asserting control over these shared spaces – not through royal decrees, but through platform architectures, lock-in effects, extraterritorial legal recourse, and sheer market power.

Because European companies were unable to find realistic alternatives for a long time, this led not only to a procurement problem – it also led to a power problem.

A new "Mare Liberum" for the digital world

At that time, *Mare Clausum* – the enclosed sea – stood in opposition to *Mare Liberum*. Europe does not want isolation or a "conflict" with American or Asian technology. It aims to prevent critical digital infrastructure from effectively remaining trapped in foreign jurisdictions. In this sense, Europe's call for digital sovereignty means the same thing that Grotius called for back then: open spaces, fair rules, and genuine freedom of choice.

A more open digital ocean for a new generation of merchants.



Course & Coordinates



Germany: A year-over-year comparison 2025/2026 – From commitment to action

A Signal Becomes a Strategy

In 2025, Germany made it clear that digital sovereignty is no longer a marginal issue. 84.4 percent of IT decision-makers said that governments and KRITIS operators should prioritize the use of European digital products. A clear signal: The market wants alternatives. 2026 will show whether this signal has evolved into a strategy: The data of this study suggests: yes.

Question 1 – European providers for KRITIS: steadfast commitment, a more nuanced approach

That fundamental conviction remains unshaken. In 2026, 87.5 percent of German IT decision-makers support the idea that KRITIS operators should prioritize European digital products – a slight increase compared to 2025.

However, the nature of consent is clearly shifting. "Rate Yes" rose from 18.3 to 40.3 percent – more than double." The percentage of undecided voters is rising moderately from 7.3 to 9.3 percent. What at first appears to be a sign of weakness is, upon closer inspection, a sign of maturity: The unqualified enthusiasm of the previous year has given way to a rational but stable consensus.

This is particularly evident at the other end of the spectrum: "No, absolutely not" has virtually disappeared, dropping from 5.5 percent in 2025 to 0.3 percent in 2026. One year after the first survey, IT decisionmakers in Germany are thus even more strongly in favor of digital sovereignty in critical infrastructure.

Question 2 – Introduction of European Software: The Market Is Experiencing a Pro-European Boom

The shift is even more pronounced when it comes to whether companies plan to adopt European software solutions. In 2025, 20.4 percent of German IT decision-makers were actively implementing the technology. By 2026, the figure will be 39.7 percent – which is nearly twice as many.

At the other end of the spectrum, the trend is just as clear. The percentage of companies that clearly reject a change has plummeted from 47.7 percent to 4.6 percent – a decline of more than 90 percent. "Don't know" fell from 17.4 to 3.9 percent.

While in 2025 many IT decision-makers were not even aware of European alternatives on, a year later they were clearly riding a pro-European tech wave on.



GERMANY

Does your company plan to implement one or more European software solutions in the future?

Period	2025	2026	Change
Already being implemented	20,4 %	39,7 %	+94,6 %
Within 6 months	3,9 %	20,4 %	+423,1 %
Within 7-12 months	5,3 %	16,8 %	+217,0 %
13-24 months	3,1 %	14,8 %	+377,4 %
No	47,7 %	4,6 %	-90,4 %
I don't know	17,4 %	3,9 %	-77,6 %

What triggered this change?

This sharp increase comes at a time when the geopolitical landscape has undergone fundamental changes. In February 2026, an article by the Reuters news agency revealed that the U.S. State Department had instructed its diplomats worldwide to actively counter efforts related to digital sovereignty.

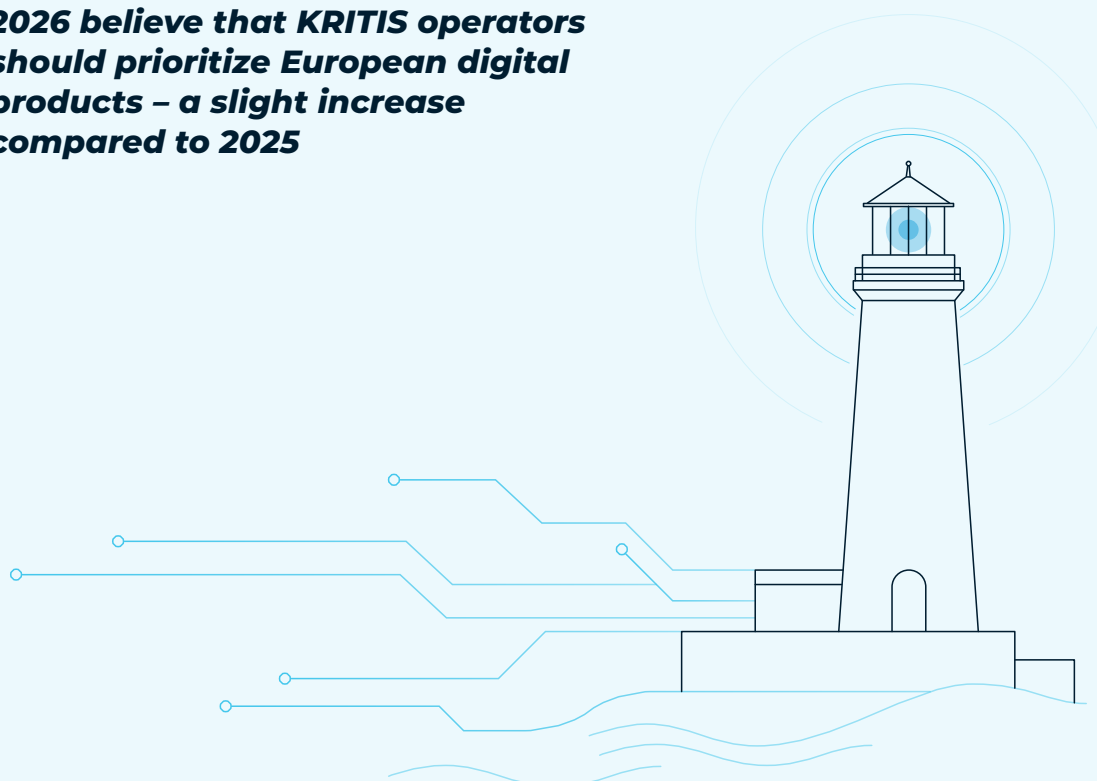
In May 2024, the International Criminal Court (ICC) in The Hague issued arrest warrants against Israeli Prime Minister Benjamin Netanyahu and then former defense minister Yoav Gallant for alleged war crimes in the Gaza Strip. In response, the U.S. government imposed sanctions on several ICC judges in the summer of 2025. As a result, their access to a number of U.S. platforms and payment services was blocked. In response, the International Criminal Court replaced its Microsoft Office software with a German solution. In June 2025, Anton Carniaux, General Counsel of Microsoft France, confirmed before the French Senate that the company would be obligated to hand over data in response to a legally valid request from U.S.

authorities – regardless of where the data is stored. He could not guarantee the protection of European user data. The CLOUD Act, which requires U.S. service providers to hand over data stored in the EU to U.S. authorities under certain conditions, suddenly became a mainstream topic.

Digital sovereignty is more than just geography. The key insight is: Data sovereignty does not depend on the server location, but rather on the provider structure, the legal jurisdiction, and operational control.

87,5 %

of German IT decision-makers in 2026 believe that KRITIS operators should prioritize European digital products – a slight increase compared to 2025



Three regions, one mission.

A comparison of Germany, France, and the Nordic countries

The same destination, three different routes

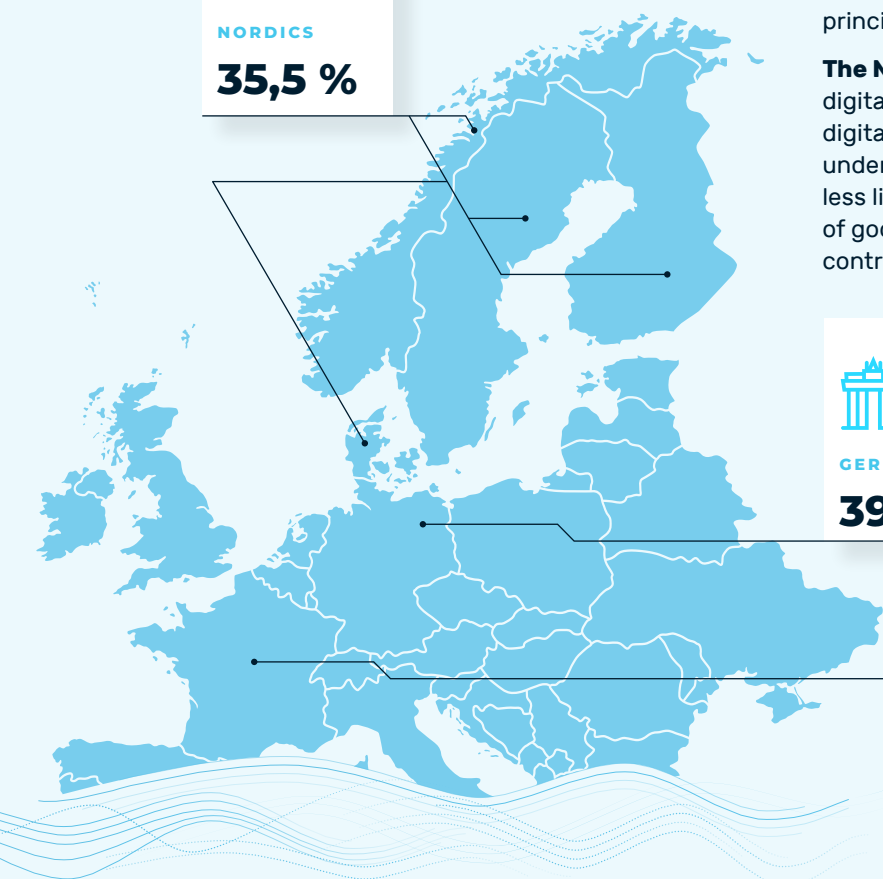
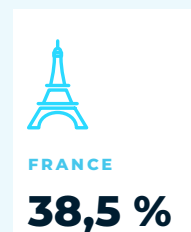
In 2026, a pattern emerges that Europe often overlooks: Digital sovereignty is not a jointly chartered ship. Each region navigates with different tools, along different routes but the destination on the horizon is the same.

Germany has its roots in industry. The state is approaching digital sovereignty from the perspectives of supply chains, critical infrastructure, and, above all, small and medium-sized enterprises. The fundamental question: How can you balance out established dependencies without jeopardizing operational stability?

France's actions are characterized by strategic autonomy. The government has traditionally played a major role in key technologies and has the capacity to act in a centralized manner. In France, digital sovereignty doesn't sound like a new buzzword, but rather like the digital extension of a well-known principle of state policy.

The Nordic countries have a background in digital practice. Characterized by a high level of digital maturity, lean administrations, and a strong understanding of security, sovereignty there seems less like an ideological concept and more like a matter of good architecture: What works, is safe, and can be controlled?

IT decision-makers who are currently switching to European technologies



Who is switching to European software, and when? A three-way comparison of implementation plans

	Germany	France	Nordics
Already being implemented	39,7 %	38,5 %	35,5 %
Within 6 months	20,4 %	17,9 %	19,9 %
Within 7–12 months	16,8 %	18,0 %	18,2 %
Within 13–24 months	14,8 %	13,3 %	16,9 %
In 25+ months	5,9 %	4,0 %	7,5 %
No	4,6 %	2,4 %	3,3 %
I don't know	3,9 %	10,1 %	5,9 %

Germany leads the way when it comes to the percentage of companies that are already actively switching to European alternatives. Across nearly all planning horizons, Nordic companies consistently rank first or second, demonstrating a consistent

willingness to change – virtually no company is opposed to change. Although France has the lowest percentage of firm opponents (2.4 percent), it also has the highest percentage of undecided voters (10.1 percent).

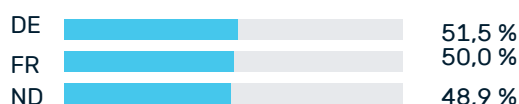
Geopolitics as a driver? How political events are changing IT strategies

The turmoil in the global order has long since reached the server rooms.

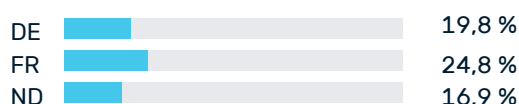
In all three regions, about half of the IT decision-makers view the increasing focus on national sovereignty as a direct consequence of geopolitical events:

In Germany, one in five IT decision-makers, and in France, one in four, say they are using more U.S. software as a result of geopolitical events

Greater Focus on National Sovereignty



Greater Use of U.S. Software



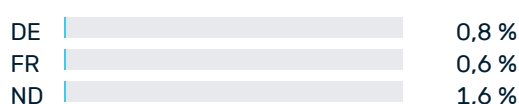
Greater Use of European Software



No changes



Don't know / No answer



In Germany, one in five IT decision-makers, and in France, one in four, report that they are using even more U.S. software as a result of geopolitical events. These figures show that headwinds do not always lead to a change of course. For companies that are heavily dependent on U.S. markets, forging closer ties to U.S. infrastructure can also serve as a protective strategy.



France: A Special Case – The Discrepancy Between Policy and Practice

Nowhere is the desire for European sovereignty over critical infrastructure more prominent than in France (93.6 percent). And yet France is the region where geopolitical events have most frequently led to an even greater use of U.S. software – and where the most IT decision-makers report that nothing has changed in their IT strategy.

Part of the explanation lies in the survey period. The survey took place from late February to early March 2026 – at a time when major political decisions in France were still pending. The announcement that Windows would be gradually replaced by Linux in the French government came only after that. This change in course is not yet reflected in the data.

IV

Shoals & Currents

Europe's new trade routes – where sovereignty is most urgent

The architecture of sovereignty

Digital sovereignty may sound abstract, but it is determined by very specific areas of technology. Which cloud infrastructure supports critical business processes? What kind of security architecture protects hospitals, energy providers, and government agencies? And on which AI systems will future decisions, automation, and value creation be based?

The survey data clearly show: When asked which technology areas they believe are most important for digital sovereignty, European IT decision-makers point to the interplay of several technological sectors. That is precisely where the new trends and interdependencies of the digital economy are emerging – and that is also where they see the need to clearly focus on efforts to ensure sovereignty. After all, if we fail to become more independent in these areas, that is where the pitfalls lie that make companies and nations vulnerable.

Cybersecurity: the common reference point

Cybersecurity is the area where all three regions are most in agreement.
Nordic countries: 68.4 percent, Germany: 57.6 percent, France: 57.1 percent.

That's not surprising. Sovereignty is determined by vulnerability. Cybersecurity is a safe haven in the digital storm – it determines whether a company can detect attacks, keep services available, protect data, and weather crises. Without security, sovereignty is merely a theoretical concept with no practical reality.

Artificial Intelligence: the Field of the Future

AI is the second major area of consensus. France leads with 52.4 percent, followed by Germany with 50.1 percent, with the Nordic countries close behind at 48.6 percent.

Cloud services: the engine room of the modern economy

47.2 percent of Nordic IT decision-makers, 46.0 percent of German IT decision-makers, and 38.1 percent of French IT decision-makers cite cloud services as critical to sovereignty.

Applications, data, AI models, customer processes – everything is increasingly running on cloud infrastructure.

Those who lack freedom of choice here lose strategic leeway: not in theory, but in daily practice.

Semiconductors and chips: Germany's industrial perspective

As a country with a long history of hardware manufacturing, IT decision-makers in Germany view the field of semiconductors and chips as significantly more critical to national sovereignty than their European counterparts do. More than one in four people (26.8 percent) in this country see a need for action in this regard – well ahead of the Nordic countries (18.6 percent) and France (18.1 percent).

The Nordics: pragmatism in depth

Nordic IT decision-makers reported the highest figures in the areas of cloud (47.2 percent), cybersecurity (68.4 percent), mobile and communications (27.7 percent), and office and business software (23.1 percent). Figures that point to a pragmatic approach: Where is data generated every day, how does it get from A to B, and who protects it?

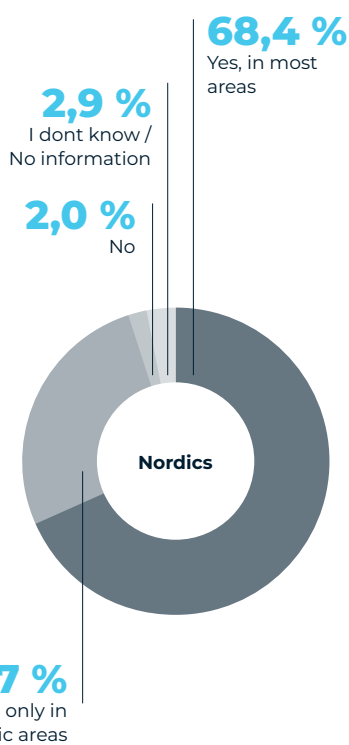
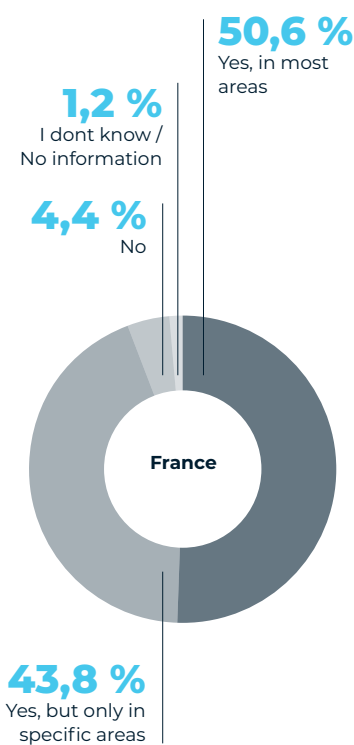
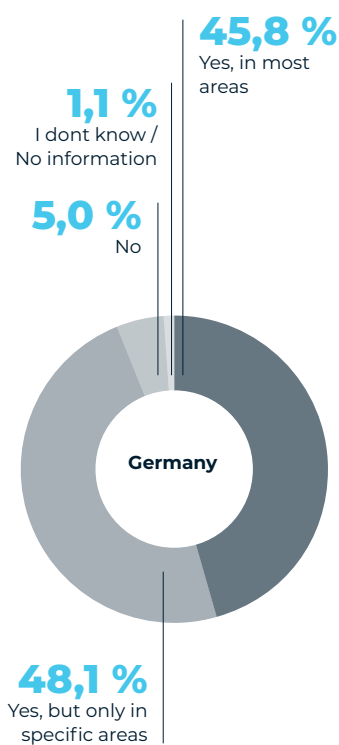
Does Europe trust itself? Confidence in European competitiveness

Europe's IT decision-makers are clearly in favor of European technologies. But behind this strategic decision lies a more fundamental question that is rarely asked aloud: Is Europe actually good enough? Anyone who wants to replace U.S. providers with European alternatives must be convinced that these alternatives not only exist but are also viable enough to secure their own digital trade routes in the long term. Otherwise, the willingness to change lacks an operational foundation.

The responses from the IT decision-makers surveyed paint a nuanced picture. The vast majority in all three regions believe that European companies are capable of developing competitive digital products. A detailed analysis of the extent of this trust – whether it is limited to individual segments or extends across large parts of the digital economy – reveals a clear north-south divide.

When the positive responses are added up, all three regions come in at around 94 to 95 percent – a strong level of basic trust. The key difference lies in the depth of confidence: More than two-thirds of Nordic decision-makers (68.4 percent) believe that Europe can achieve digital sovereignty “in most areas.” In doing so, they demonstrate a broad, confident faith in European technology. IT executives from Germany and France share this underlying optimism, but a larger proportion of them lean toward the more cautious stance of “Yes, but only in certain areas.”

But: The foundation for a credible European technological breakthrough already exists among a broad range of decision-makers. What is missing is not conviction, but rather flagship projects and best-practice examples that can translate general trust into concrete decisions.



Europe's complementary strengths

The three different priority profiles complement each other very well: Germany brings hardware expertise and industrial depth to the table. France brings AI ambitions and a strategic drive to shape the future. The Nordics bring cloud expertise, a culture of cybersecurity, and a pragmatic approach to implementation.

Europe, which was founded as a community after all, does not need individual levers of sovereignty. It simply needs to bring these complementary strengths together if it wants to have a European architecture.

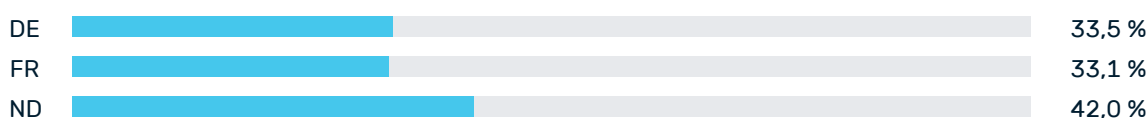
The challenges of migration: why changing course remains difficult – but is feasible

Over the years, many companies and institutions have built up software landscapes that have grown like fleets: Plank by plank, deck by deck, with deeply ingrained routines and crews who have been operating

the same instruments for decades. No one can retrofit fleets like that overnight. However, there is broad consensus that they must adapt in light of the changing times.

The challenges of switching to a three-way comparison of European IT solutions

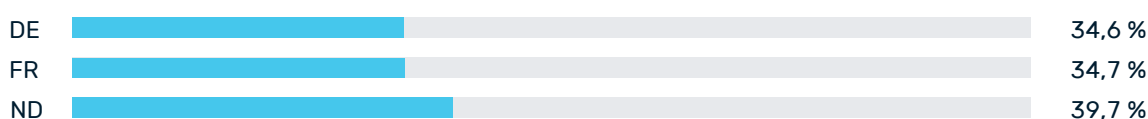
Lack of information about European alternatives

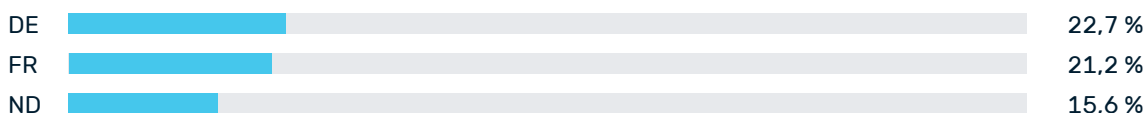
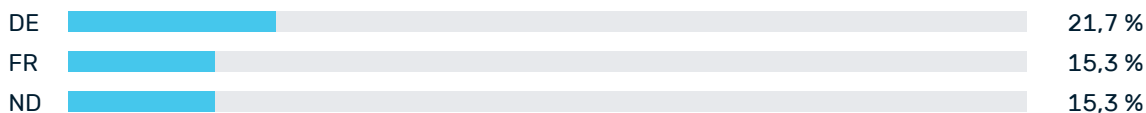
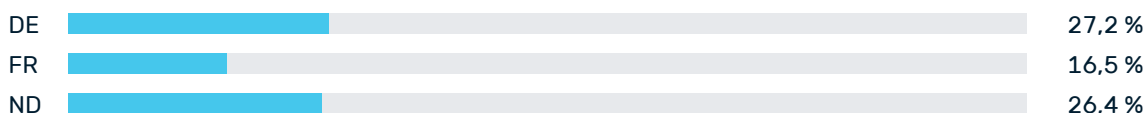
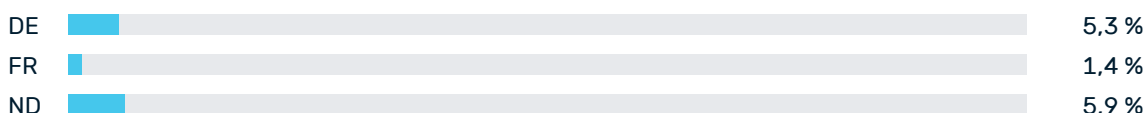
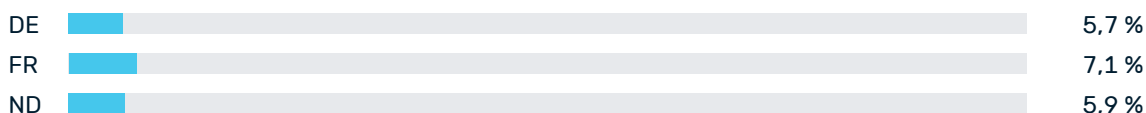
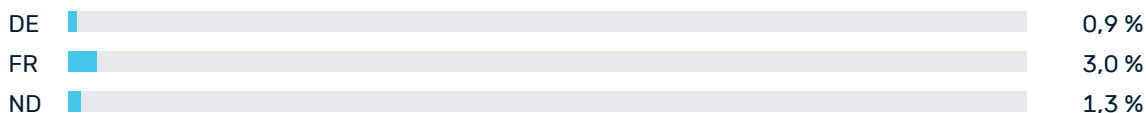


Inadequate technical performance



High migration costs



Lack of perceived urgency**Internal Resistance / Politics****Lack of integrability****Other****No obstacles present****I don't know****Migration costs – real, but not the main factor**

High migration costs are among the most frequently cited barriers to switching to European IT solutions in all regions. And yet: About two-thirds of German IT decision-makers do not view it as a serious obstacle. In France, too, the proportion of people who do not view migration costs as an obstacle is around 65 percent; in the Nordic countries, it is about 60 percent. The costs are real, but for the majority, they are not a reason not to change course.

If you're not visible, you won't be procured – and if you aren't procured, you'll grow more slowly

Information gaps – visibility is a strategic factor

A lack of knowledge about European alternatives is holding back 42.0 percent of IT executives in the Nordic countries, 33.5 percent in Germany, and 33.1 percent in France. Conversely, this means: In all three regions, the majority of IT decision-makers are not held back by a lack of information. However, a good alternative isn't much help if it doesn't make the shortlist. Otherwise, this leads to a market problem with a self-reinforcing mechanism: If you're not visible, you won't be procured – and if you're not procured, you'll grow more slowly. Marketplaces, certification frameworks, and targeted communication are no small matter when it comes to building a new sovereign infrastructure.

A clear majority believes in Europe's technical capabilities

Only 24.4 percent of Nordic IT decision-makers cite inadequate technical performance as a barrier to switching three-quarters have no technical reservations. This is consistent with the Nordic countries' strong confidence that they will be able to

decisionachieve digital sovereignty to a large extent over the next 10 years. In Germany, nearly one-third (31.0 percent) of people have doubts about the technical capabilities. Conversely, however, this also means that 69.0 percent do not.

Do IT decision-makers view the use of European software as a business risk?

	Germany	France	Nordics
Yes, high risk	14,8 %	15,9 %	16,6 %
Yes, low risk	58,8 %	55,1 %	62,2 %
No risk	23,4 %	24,6 %	16,6 %
Yes, combined	73,6 %	71,0 %	78,8 %

The fact that the Nordic countries perceive the highest combined migration risk (78.8 percent) is not a contradiction to their determination – it is the flip side of it. Anyone who is familiar with complex IT transitions and yet decides to change course does so not out of naivety, but out of a calculated decision. French IT decision-makers are the most optimistic in Europe: One in four (24.6 percent) sees no risk whatsoever in switching to European solutions.

Anyone who is familiar with complex IT transitions and yet decides to change course does so not out of naivety, but out of a calculated decision

The CLOUD Act as a warning sign – between waiting and taking action

A law that makes borders visible

The Clarifying Lawful Overseas Use of Data Act – or CLOUD Act for short – was enacted in the United States in 2018. It requires U.S. technology companies to grant U.S. authorities access to stored data upon request – regardless of where in the world that data is physically located. A server in Frankfurt, operated by a U.S. provider, is therefore potentially subject to U.S. jurisdiction. This creates a structural dependency for European companies: The GDPR is

intended to protect personal data under European law; at the same time, the CLOUD Act establishes a parallel, extraterritorial right of access that can effectively undermine this protection. Companies must therefore comply with European data protection standards, but at the same time remain vulnerable to external access that they can neither control nor reliably prevent.

How is Europe responding? A comparison of specific measures

What measures is your company taking in response to the CLOUD Act, which requires U.S. service providers to hand over data stored in the European Union to U.S. authorities?

Maßnahme	Germany	France	Nordics
See no need for action	5,0 %	6,1 %	3,6 %
Changed providers	16,4 %	18,5 %	13,3 %
Planning to switch providers	32,4 %	21,0 %	28,7 %
Benefits of Stronger Encryption	34,6 %	27,0 %	30,9 %
Monitor further developments	47,6 %	39,1 %	51,8 %
No special measures	3,9 %	7,3 %	3,6 %
The CLOUD Act was not known	1,7 %	4,0 %	2,6 %
Don't know / No answer	2,7 %	4,8 %	3,6 %

When it comes to dealing with the CLOUD Act, Germany and the Nordic countries are the most willing to take action: 32.4 percent of German IT decision-makers plan to switch providers, and 16.4 percent have already done so. Although 18.5 percent in France have already switched providers – the highest figure among all three regions – only a few IT executives are planning to take further steps. Only 3.6 percent of Nordic IT decision-

makers see no need for action – compared with 5.0 percent in Germany and 6.1 percent in France. The fact that only a tiny minority of respondents are unfamiliar with the CLOUD Act – with the figure not exceeding 4.0 percent in any of the three regions – shows one thing above all: The issue has finally made its way to the top echelons of European IT decision-makers.

The CEO letter: warning against sovereignty washing

This trend is also evident in the European cloud industry. In April 2026, 25 CEOs of European cloud and digital companies warned the European Commission against defining digital sovereignty too broadly. Their open letter regarding the proposed Cloud and AI Development Act is directed against a practice that the industry has come to call “sovereignty washing.”

This refers to proposals that promise European control but perpetuate central dependencies. Providers advertise their data centers in the EU, local subsidiaries, or product names that sound prestigious. At the same time, corporate structures, administrative rights, technical controls, and legal access paths outside Europe remain in place.

What data sovereignty really means – three levels of control

The debate over digital sovereignty has fundamentally changed the way we view data sovereignty. Nowadays, simply having a server location in Frankfurt or Stockholm is hardly considered sufficient proof of sovereign data processing. Questions regarding actual control, dependencies, and the ability to act are increasingly taking center stage: Who manages the systems and keys? Which jurisdictions apply in an emergency? And to what extent can an organization remain independent of providers and platforms?

Against this backdrop, several European countries are developing political and organizational approaches aimed at making digital sovereignty more operational. In Germany, the Center for Digital Sovereignty in Public Administration (ZenDiS) develops criteria and evaluation methods for sovereign IT in public administration. In particular, the focus is on the ability to switch providers, flexibility, and the ability to influence providers as strategic goals of digital sovereignty. In France, the Direction interministérielle du numérique is pursuing a similar approach with “La Suite Numérique” to provide government-coordinated, open-source administrative tools. The two institutions have also been collaborating at the institutional level since 2024.

This study therefore examines data sovereignty across three levels of control:

Technical Inspection: Who manages the encryption keys? Who has access to logs, backups, identities, and administrative interfaces? Technical control means that no external party can access data without the operator's knowledge and consent.

Legal Review: What law applies to the provider, its parent company, and access to data in the event of a crisis? Parallel jurisdictions under foreign legal systems – such as those arising from extraterritorial laws – must not exist if true data sovereignty is to be achieved.

Operational Control: In the event of a crisis, can a company take action – switch, isolate, or continue operations? Operational control means that systems are designed in such a way that switching and exit scenarios can be realistically tested and implemented without jeopardizing business operations.

Today, a server location in Frankfurt or Stockholm alone is hardly considered sufficient proof of sovereign data processing

The U.S. Dispatch – when dependence takes on a political face

In February 2026, Reuters revealed in an article that the U.S. State Department had instructed its diplomats worldwide to oppose data localization and digital sovereignty laws. What began as a technical dependency has thus become an openly declared geopolitical agenda. For European IT decision-makers, this means a shift in risk perception: Dependence on U.S. infrastructure is thus no longer

merely a matter of neutral procurement decisions, but also a potential gateway for external pressure.

The CLOUD Act itself is like a bolt of lightning in the night sky. A potential danger that can strike at any moment and bring to light things that are actually meant to remain hidden.

V Horizon



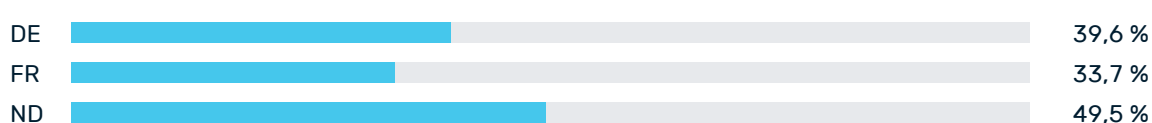
Eyes on the Horizon – how realistic is digital independence by 2035?

The assessment in a three-way comparison

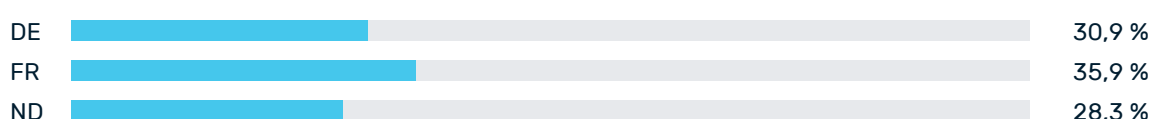
Complete digital independence



A high degree of digital independence



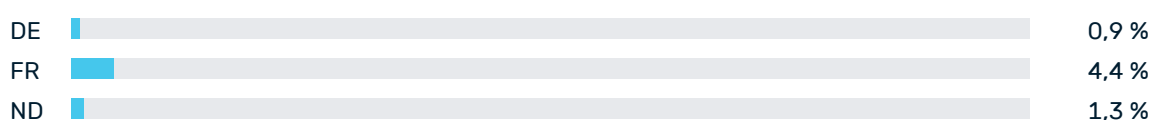
Independence in key areas



Only a slight reduction in dependencies



No change



Don't know / No answer



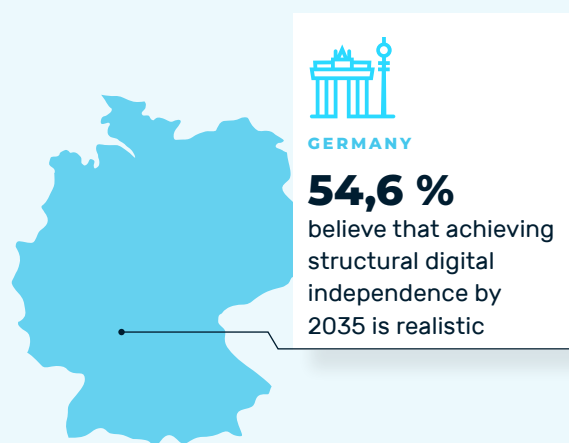
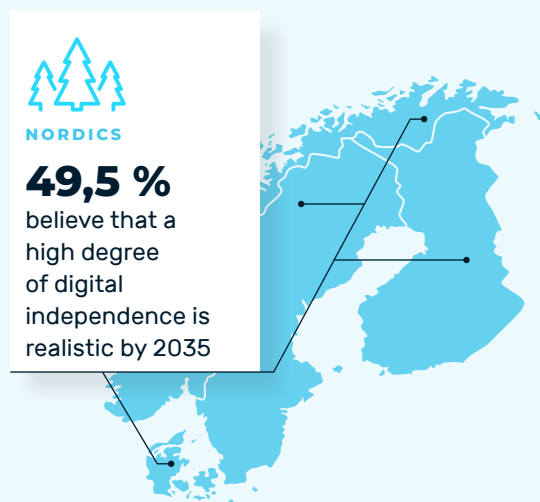
Any improvement (combined)



Nordics: Optimism Backed by Substance

49.5 percent of Nordic IT decision-makers believe that achieving a high degree of digital independence by 2035 is realistic – the only figure that comes close to the 50 percent mark. Another 15.0 percent even believe Europe is capable of achieving complete independence. Overall, 64.5 percent of Nordic IT decision-makers believe that Europe can achieve structural self-sufficiency in ten years.

This optimism doesn't come out of nowhere. The Nordic countries have undergone digital transformation earlier and more thoroughly than most other European regions. Anyone who has seen how quickly a society can transform its digital infrastructure is more likely to believe that it can do so again.

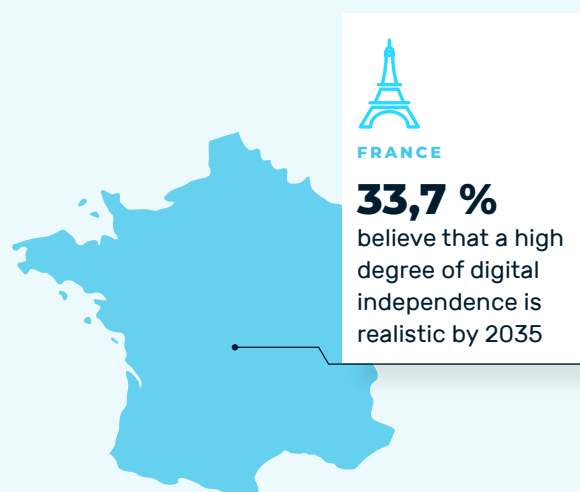


Germany: cautious optimism

54.6 percent of German IT decision-makers believe that Europe can achieve greater structural autonomy by 2035. Nearly one in four (39.6 percent) considers extensive digital independence to be realistic: a sector-specific optimism that points to the wellknown German tendency to break down major transformations into manageable subprojects.

France: realism with potential

Overall, France is the most pessimistic: Only 33.7 percent consider a high degree of independence to be realistic, and 6.2 percent do not believe there will be any change at all – the highest figure among all regions. But a closer look reveals that, when it comes to independence in key areas, France actually leads the way with 35.9 percent. France thinks in terms of priorities—not in absolutes.



Conclusion: Europe does not need to own the digital ocean. But it has to be able to navigate on its own again.

A Europe that has become more alert

This study shows a Europe on the move. Not a sprint – but a decisive change of course.

IT decision-makers in Germany, France, and the Nordic countries have embraced digital sovereignty as a strategic priority. They adapt IT strategies. They are planning migrations. They invest in European software. They see risks – but they don't hide behind them.

Germany is sending a strong message: The percentage of companies that have already adopted European software has nearly doubled within a year. The percentage of those who categorically reject a change has plummeted from 47.7 to 4.6 percent. Not just minor shifts, but structural change in real time.

The percentage of companies that have already adopted European software has nearly doubled within a year

What the Three Regions Teach Us

Germany is taking a thorough and risk-conscious approach. The state brings industrial depth and expertise in critical infrastructure to the table. The hurdles are real – high migration costs, complex IT environments, and the need for internal consensus. But the bow has turned.

France approaches sovereignty strategically and with political momentum. The data reveal a strong claim to sovereignty, but also hesitation in its operational implementation. However, France's most recent political decisions leave no doubt that it has found its new direction.

The Nordic countries are Europe's pragmatic pioneers. A high level of digital maturity, a broad willingness to embrace change, coupled with strong confidence in Europe's competitiveness. The Nordic countries show where things can go – when pragmatism and digital culture come together.

Together, these three strengths can form a European route: Germany supplies industrial foundations. France demonstrates political will, and showcases its AI ambitions. The Nordics bring digital maturity and implementation experience.

What would have to happen? Five lines of action



48° 08' 24.2" N
11° 31' 19.8" E



The Grotius question rephrased

Hugo Grotius did not write *Mare Liberum* because he loved conflict. He wrote it because he realized that shared spaces without fair rules become instruments of power.

Europe faces the same fundamental question today. It seeks the digital equivalent of what Grotius called for back then: open spaces, fair rules, and genuine freedom of choice. The digital ocean must not belong to just a few. It must remain open, secure, and accessible to all.

Europe does not have to own this sea. But it has to be able to navigate on its own again. The most important thing now is not only to take advantage of the tailwind from European IT decision-makers and take the helm, but above all to stay the course.

Nicholas of Myra – Patron Saint of sailors and merchants, and a beacon of digital sovereignty

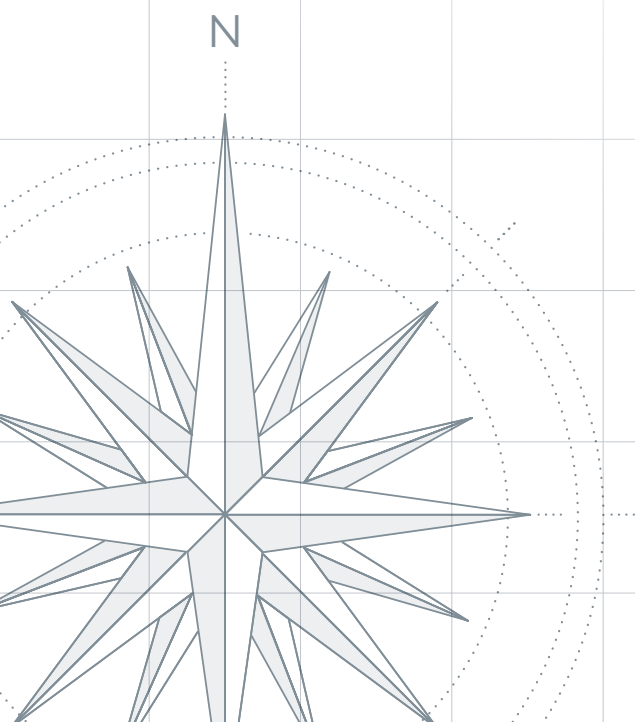
Myra was a port city on the southern coast of Asia Minor, in present-day Turkey. St. Nicholas, a fourth-century bishop, became the patron saint of sailors and merchants.

Those who shipped goods via unsafe routes, those who engaged in long-distance trade, sought guidance and trust in his name.

In the past, maps, lighthouses, and ports determined the success of a trading voyage. Today, security architecture, data sovereignty, and the choice of the right infrastructure are the deciding factors. For Myra Security, the mission remains the same:

Safety on unsafe roads. Reliability when it counts.

Nicholas of Myra protected those who set out on their journeys. Myra Security protects those who navigate the web.



Myra State of Digital Sovereignty 2026 (Digital version of the study + supplementary material)

Scan the QR code to access the digital version of the study, as well as supplementary materials and additional information.



Methodological Note:

The results are based on a Civey survey commissioned by Myra Security and conducted among 1,818 IT decision-makers in Germany (1,007), France (504), and the Nordic countries – Denmark (76), Norway (76), Sweden (78), and Finland (77) – and was conducted between February 25 and March 5, 2026. The survey was conducted online; for questions allowing multiple responses, respondents could select more than one category. The statistical margin of error is approximately ± 5 percent. Digital sovereignty is defined here as the ability to rely on European software solutions rather than being dependent on non-European providers.

Note on Language and Gender Inclusion:

For the sake of readability, this report uses the generic masculine form. All references to people apply equally to all genders – unless explicitly stated otherwise.

Made in Germany



Myra protects what matters most. In the digital world.

Would you like to learn more about how our solutions can help you increase your revenue, minimize your costs, and protect your applications from malicious attacks? Our team of experts will be happy to provide you with personalized advice and develop a customized solution for your organization. We recommend that you schedule a no-obligation consultation today.

Cyberattacks are expensive, but a no-obligation consultation costs nothing.

Myra Security GmbH

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