

Data Sovereignty 2026: Reality, Relevance, Roadmap

BARC Topical Survey

Research sponsored by



In cooperation with



Authors



Dr. Carsten Bange | Founder & CEO

As founder and CEO, Dr. Carsten Bange has built BARC into Europe's leading market analysis and consulting firm for data & analytics over the past 25 years. With his team of 50 people, he helps companies make the strategic, organizational and technological decisions that ensure their successful transformation into data- and analytics-driven organizations.

Dr. Bange is considered one of the leading experts on the technology market and the beneficial use of data & analytics, which makes him a sought-after speaker, author and consultant for companies, software vendors and service providers as well as investors.

Contact

Mail: cchange@barc.com

www.barc.com

Social Media:

[LinkedIn](#)



Timm Grosser | Senior Analyst Data & Analytics

Timm Grosser is a Senior Analyst Data & Analytics at BARC with a focus on data strategy, data governance and data management. His core expertise is the definition and implementation of data & analytics strategy, organization, architecture and software selection.

He is a popular speaker at conferences and seminars and has authored numerous BARC studies and articles.

Contact

Mail: tgrosser@barc.com

www.barc.com

Social Media:

[LinkedIn](#)

Table of Contents

Executive Summary	5
Survey Results	8
Data Sovereignty Has Become a Strategic Imperative	9
North America Rates Sovereignty Higher	12
External Drivers Are Shifting From “Rules” to “Risk”	14
Internal Drivers: Data and AI Are Raising the Stakes	16
Maturity: Ambition Is High, Execution Is Uneven	18
Sovereignty Becomes Real: Security First, Cloud Strategy in Transition	20
Challenges: People Issues Continue – While Technical Hurdles Surge in 2026	24
Recommendations	26
Methodology	29
About BARC	31
Sponsor Profiles	33
Action	34
Exasol	35
STACKIT	36
T-Systems	37
Collaboration Partner	38
Big Data & AI World Frankfurt	39



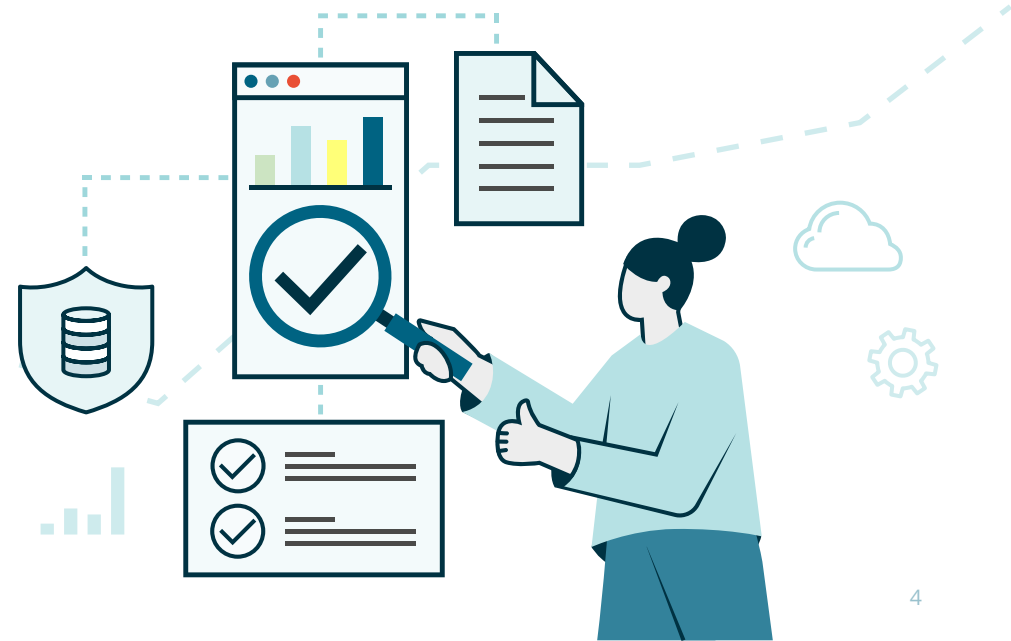
Foreword

Data sovereignty has moved from specialist topic to board-level issue. In 2026, organizations no longer discuss sovereignty only as a compliance requirement, but as a strategic condition for running data- and AI-driven core processes without taking unacceptable risk.

This is the second edition of our survey on data sovereignty and provides valuable insight into how perceptions of sovereignty – and its practical implications – have changed over the last year.

This report summarizes the key results of our 2026 data sovereignty survey and interprets what they mean for strategy, operating models, and architecture decisions. It focuses on the practical tension we see in many organizations: sovereignty is rated as highly important, but the path from intent to execution remains uneven.

Dr. Carsten Bange, Timm Grosser
April 2026



Executive Summary





1 Highlight – Data sovereignty is now “very important” for the majority, and the trend is still rising

Importance increased again from 2025 to 2026: 51% now rate data sovereignty as *very important** (up from 42%), and 89% rate it as *very** or *rather** important overall. Only 2% say it is not important. Regulated industries continue to lead, with 69% rating sovereignty as very important. Looking ahead, momentum remains strong: 76% expect its importance to increase further, and almost nobody expects a decline.

2 Highlight – Sovereignty has shifted from principle to strategy, but not everyone invests accordingly

Data sovereignty has become a strategic imperative. Almost one in three organizations has anchored it as a core part of the data or digital strategy, and another one in three addresses it selectively through initiatives. At the same time, a substantial share still treats sovereignty as a topic that “happens implicitly” or is addressed only within existing projects. The result is a split between organizations that translate sovereignty into dedicated programs and those that keep it mostly at the level of intention.

3 Highlight – North America is more convinced, and funding patterns show more action

A regional comparison reveals a clear gap in urgency and execution. In North America, 62% rate data sovereignty as very important, versus 48% in Europe and 47% in the rest of the world. Funding patterns reinforce the picture: across all respondents, 40% have not invested in sovereignty initiatives at all, only 10% have a dedicated budget, and 49% fund it within existing projects. In North America, 73% fund sovereignty either through dedicated budgets (16%) or within existing budgets, while the comparable share in Europe is 56% (with 9% having a dedicated budget).



4 Highlight – Regulation still dominates as a driver, but “risk” is catching up

External drivers remain led by legal and regulatory requirements, named by 61% in 2026 (down from 69% in 2025). At the same time, other risk-related drivers grew: political developments in the US increased from 46% to 54%, cybersecurity from 42% to 49%, and concern about dependency on public cloud offerings from 40% to 46%. The sovereignty discussion is becoming less one-dimensional: compliance remains the baseline, but resilience and dependency risk are increasingly shaping priorities.

5 Highlight – Execution lags behind ambition, especially for governance and architecture depth

When organizations benchmark maturity against the high importance they assign to sovereignty, gaps become visible. 46% report a fully established or well-defined technical architecture, 44% report strategic alignment, and 38% report applied governance. Organizations that have anchored sovereignty in strategy feel substantially better prepared, but even “doers” show uneven maturity across the three pillars. This signals that many programs start with intent and funding but still struggle to institutionalize governance and architecture patterns.

6 Highlight – The people factor remains a top barrier, and technical hurdles surged in 2026

The top challenges remain human and organizational: lack of human resources (44%), lack of internal expertise (more than a third), and organizational challenges (30%). However, 2026 reveals a notable shift: technical hurdles increased sharply as a perceived challenge from 26% to 43%, with legacy integration named by about one third. This reflects a reality check: as more organizations move from policy discussion to architectural implementation, integration constraints and legacy complexity become harder to ignore.

Survey Results



Survey Results

Data Sovereignty Has Become a Strategic Imperative



Importance Jumped Again in 2026, and Regulated Industries Are Setting the Pace

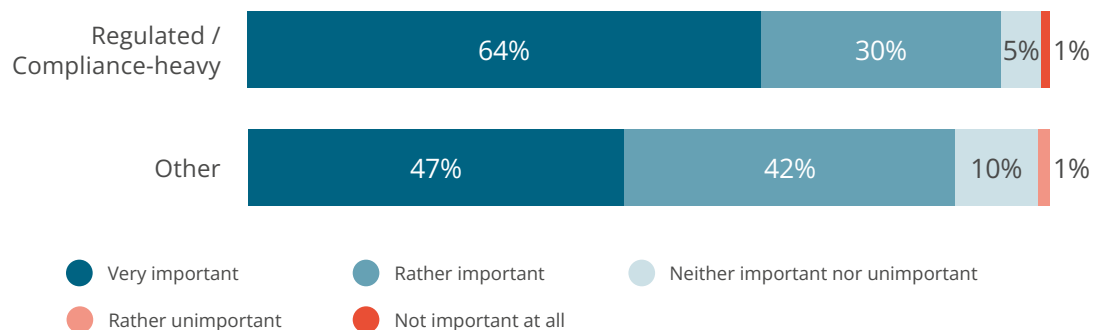
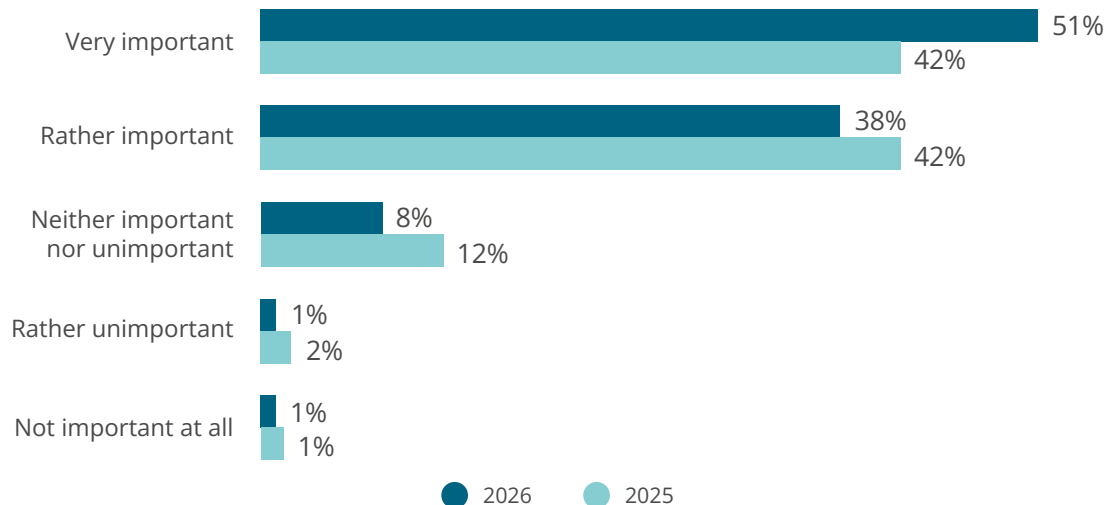


Figure 1: How important is data sovereignty for your company at the moment? (n₂₀₂₆=320 | n₂₀₂₅=291)

Figure 2: How important is data sovereignty for your company at the moment? By industry (n=320)

Viewpoint



The importance of data sovereignty was already highly regarded in 2025 and has grown even further in 2026: 51% of respondents now say it is very important, compared to 42% last year. Across the full sample, sovereignty is broadly relevant: 89% consider it very or rather important, and only 2% say it is not important.

Regulated industries are ahead of the average, with 64% rating sovereignty as very important. This is consistent with the long-standing reality that regulated sectors have faced stronger constraints on data handling, auditability, and risk management. However, non-regulated industries are now increasingly moving in the same direction, driven by data and AI use in core processes and by growing concerns around technology dependency.

The key shift is not only greater awareness, but a change in the “default assumption.” For many organizations, sovereignty is becoming a requirement for scaling data and AI, rather than a constraint that can be negotiated case by case.

Organizations Now Treat Sovereignty as Strategy, Not Just Compliance

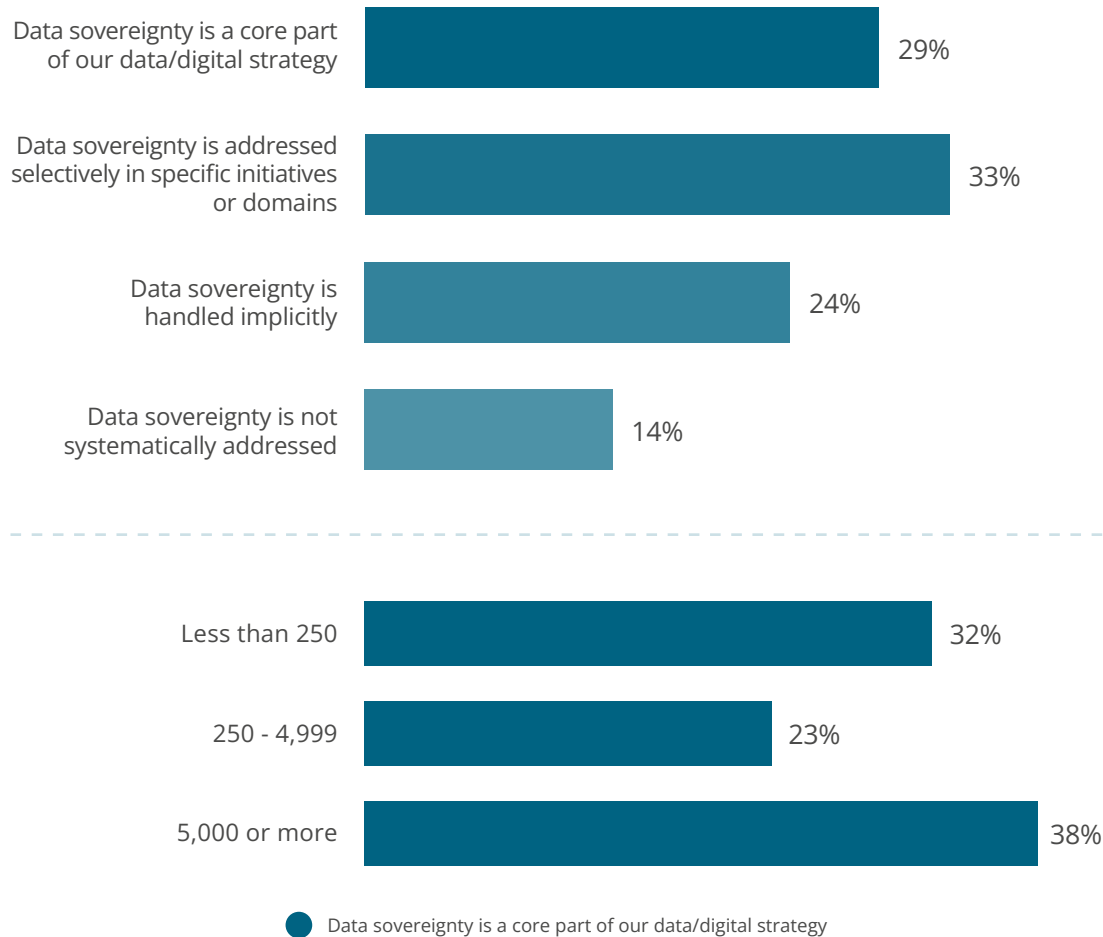


Figure 3: Which of the following best describes your company's current approach to data sovereignty? (n=315)

Figure 4: Which of the following best describes your company's current approach to data sovereignty? By company size (n=315)

Viewpoint



Data sovereignty has become a strategic imperative. Almost one in three organizations has anchored it as a core part of its data or digital strategy, and another one in three addresses it selectively through initiatives. A further 25% report that they address sovereignty only implicitly – which may indicate maturity (because sovereignty is already embedded) or, alternatively, that it is not being made an explicit priority.

Only 14% of organizations say they do not address data sovereignty at all. This matters because it shows the topic has moved beyond compliance teams and is increasingly shaping cloud strategy, architectural patterns, vendor selection, and operating model decisions. The strategic anchoring is particularly pronounced among large companies (38%) and small companies (32%), while mid-sized organizations (23%) lag behind and more often handle sovereignty as a requirement within existing projects rather than as an explicit strategic program.

Mid-sized organizations often face the hardest trade-off. They have enough complexity and exposure to sovereignty risks to feel the pressure, but they rarely have the capacity to run dedicated sovereignty programs. This is exactly where pragmatic patterns and governance standardization can create disproportionate value.

Survey Results

North America Rates Sovereignty Higher



North American Respondents Rate Sovereignty "Very Important" Far More Often Than the Rest of the World

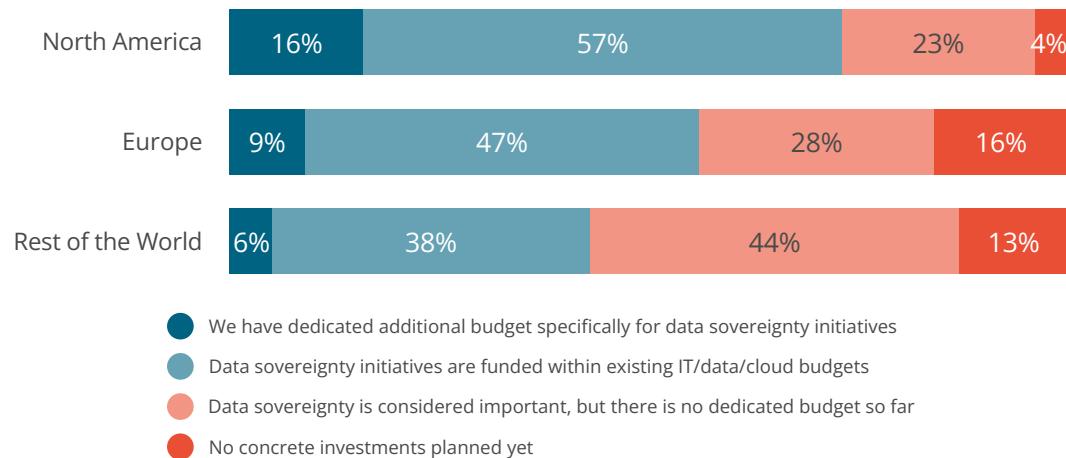
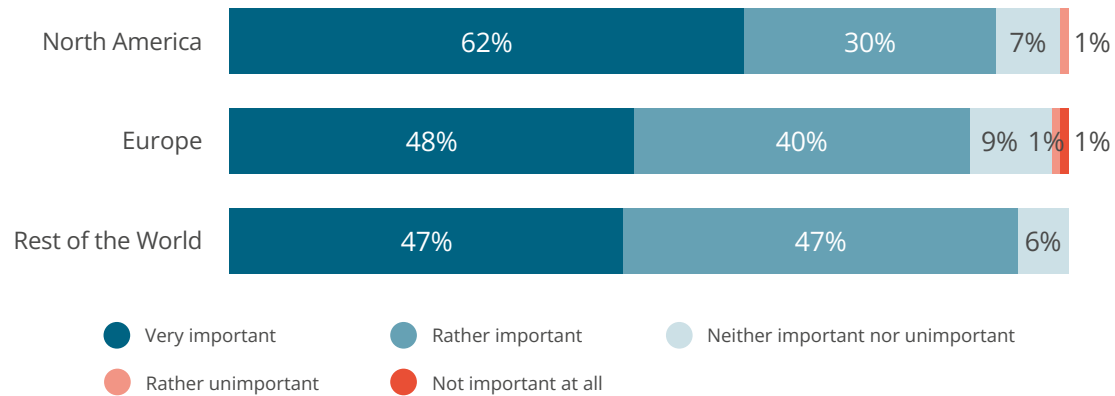


Figure 5: How important is data sovereignty for your company at the moment? By region (n=320)

Figure 6: How are data sovereignty initiatives funded in your company? By region (n=299)

Viewpoint



Regional differences are pronounced. In North America, 62% rate data sovereignty as very important. In Europe, the share is 48%, and in the rest of the world 47%.

Part of the difference can be explained by different market dynamics and technology dependencies. North American organizations typically operate closer to the ecosystems that define the dominant public cloud and AI innovation trajectories. As a result, dependency risks can be managed more proactively and the risk that a foreign government or foreign companies will gain access to one's own data is significantly lower. European organizations, in contrast, may have a stronger default expectation that regulation will "set the rules", but they often translate this into slower execution on architecture and funding.

Europe does not lack awareness but the gap is more visible in how quickly organizations convert awareness into funded execution, measurable maturity, and architectural patterns.

North American organizations fund sovereignty, while many European peers still absorb it into "business as usual"

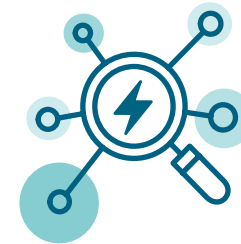
Funding patterns reveal a structural execution gap. Across all respondents, 40% are not investing in sovereignty initiatives at all. Only 10% have a dedicated budget, while 49% fund sovereignty within existing projects.

In North America, the picture is different: 73% fund sovereignty either through dedicated budgets (16%) or within existing budgets. In Europe, the comparable share is 56%, with only 9% reporting a dedicated budget. This supports a practical interpretation: North American organizations more often behave like "doers," while many European organizations remain "talkers" discussing sovereignty as important but not consistently resourcing the implementation work.

Funding is not only a financial decision. It is a signal that sovereignty is treated as a program with accountable outcomes rather than as a side requirement attached to other initiatives.

Survey Results

External Drivers Are Shifting From "Rules" to "Risk"



Regulation Still Dominates, but Dependency and Cybersecurity Concerns Are Catching Up

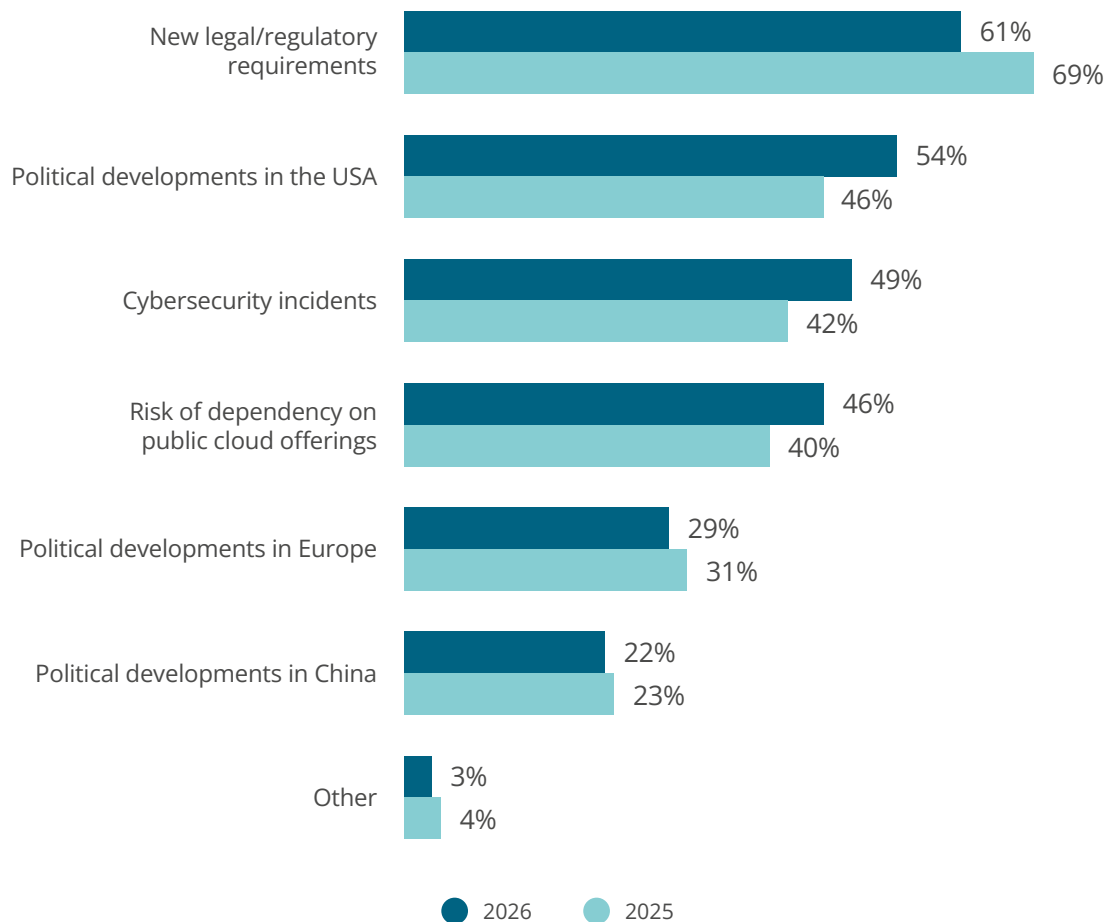


Figure 7: Which external factors have made data sovereignty more relevant for your company?
(n₂₀₂₆=316 / n₂₀₂₅=293)

Viewpoint



Legal and regulatory requirements remain the top external driver for sovereignty initiatives, but their dominance is slowly decreasing: 61% cite regulation in 2026, down from 69% in 2025.

At the same time, other drivers have gained momentum: political developments in the US rose from 46% to 54%, cybersecurity from 42% to 49%, and concern about dependency on public cloud providers from 40% to 46%.

This pattern indicates that sovereignty is no longer seen purely as a “must do” response to rules. It is increasingly framed as risk management across cybersecurity, cloud provider dependency, and geopolitical uncertainty. That framing matters, because it pushes sovereignty discussions into enterprise architecture, vendor strategy, and resilience planning.

When sovereignty is treated only as compliance, governance becomes the primary tool. When it is treated as dependency risk, architecture choices and portfolio strategy become equally important.

We also observed some interesting differences between companies that have a dedicated budget for data sovereignty initiatives and the rest: While all companies view new legal and regulatory requirements and political developments in the US as major drivers of the issue’s growing relevance, companies with a dedicated additional budget cite political developments in Europe (48%) and cybersecurity incidents (68%) as relevance drivers significantly more often.

Survey Results

Internal Drivers: Data and AI Are Raising the Stakes



Increased Operational Use of Data and AI Drives Sovereignty Relevance

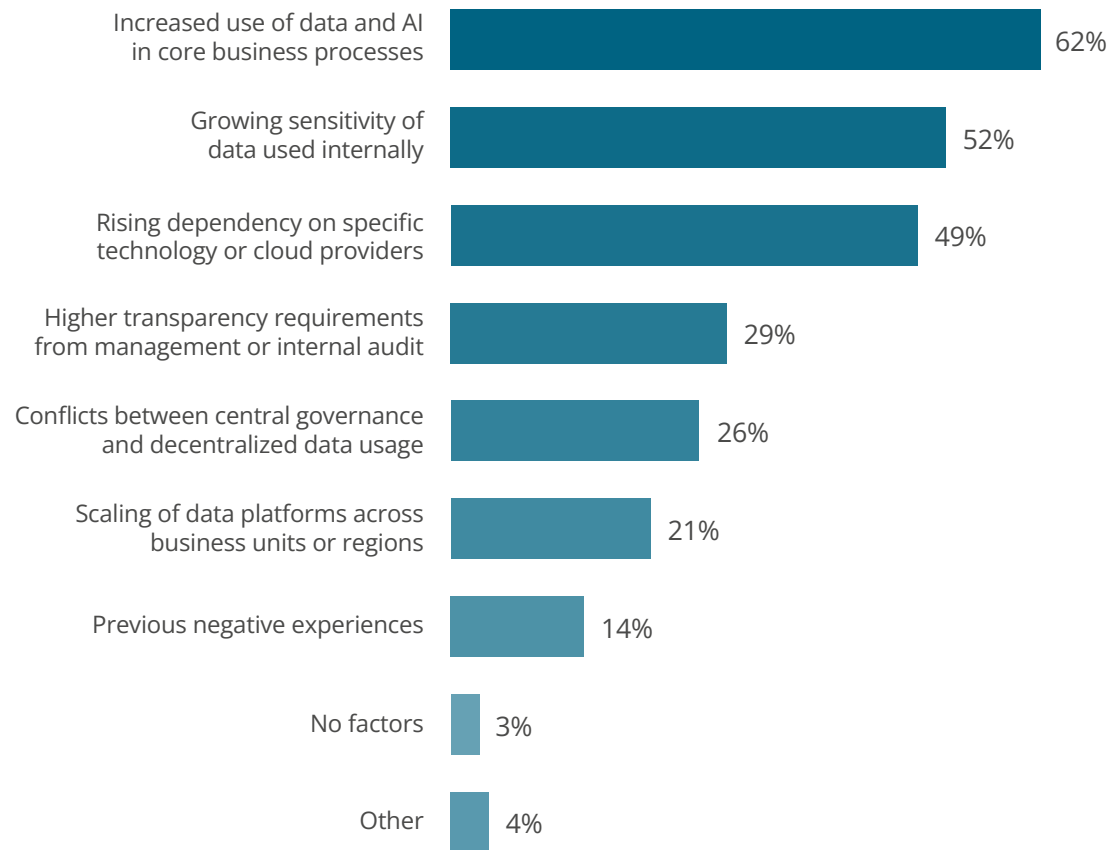


Figure 8: Which internal factors have made data sovereignty more relevant for your company? (n=318)

Viewpoint



Internal drivers for data sovereignty cluster around three forces.

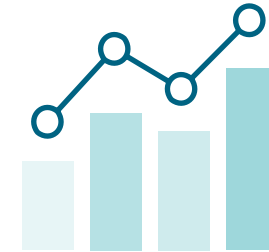
1. **62%** cite the increased use of data and AI in core business processes as a key reason why sovereignty has become more relevant
2. **52%** state that the sensitivity of the data used is increasing – reflecting a broader realization that data is a key differentiator versus competitors
3. **49%** mention increasing dependency on specific technology or cloud providers

These forces reinforce each other. As organizations run more critical processes on data and AI, the value of context, lineage, and control increases. At the same time, the downside of dependency rises, especially when operational continuity, auditability, and control over data processing become central to competitiveness.

The sovereignty debate is increasingly about operating core business safely at scale. The more data and AI initiatives move from experimentation to production, the less tolerance organizations have for unclear control boundaries and risk exposure.

Survey Results

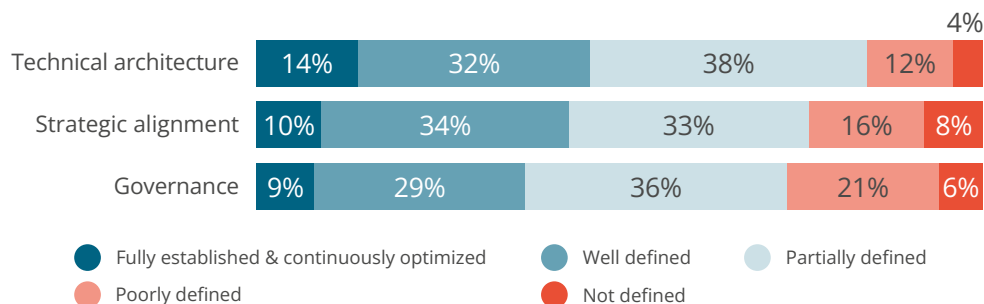
Maturity: Ambition Is High, Execution Is Uneven



Overall Data Sovereignty Maturity Is Limited – Companies with Dedicated Budget Excel in Strategic Alignment



Maturity data shows a consistent pattern. 46% report a fully established or well-defined technical architecture. 44% report a fully established or well-defined strategic alignment. 38% report applied governance. 38% report applied governance.



Enterprises with dedicated sovereignty budget



Enterprises with a sovereignty strategy



Figure 9: Please rate your organization's maturity in the following aspects of data sovereignty (n=317)

Figure 10: Please rate your organization's maturity in the following aspects of data sovereignty. By investment mode (n=298)

Figure 11: Please rate your organization's maturity in the following aspects of data sovereignty. By approach (n=271)

Organizations that anchor sovereignty as a core part of strategy achieve a significantly higher maturity, with 81% reporting strategic alignment, 68% governance, and 70% technical architecture. Among those with dedicated budgets, 75% report well-defined or fully established strategic alignment, but only 48% report well-defined governance and 54% report well-defined or fully established technical architecture.

Many programs start with strategy work because it is easier to initiate, align, and communicate. Governance and architecture maturity require operationalization, standardization, and sustained implementation capacity. That is where many organizations hit friction.

Regional maturity differences mirror the earlier reported funding patterns. 57% of North American respondents report fully established or well-defined strategic alignment versus 40% in Europe. Governance shows a smaller gap: 42% in North America versus 37% in Europe, suggesting that many European organizations have frameworks and intent. Technical architecture shows the strongest difference: 64% in North America versus 41% in Europe. This suggests that implementation patterns, platform decisions, and integration execution remain the bottleneck for European companies.

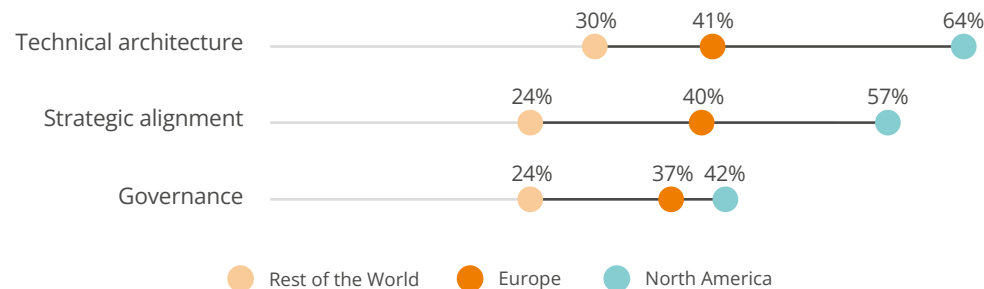


Figure 12: Please rate your organization's maturity in the following aspects of data sovereignty. By approach and region (n=317)

Survey Results



Sovereignty Becomes Real: Security First, Cloud Strategy in Transition

Security and Cloud Strategy Adaptation Dominate the Action List

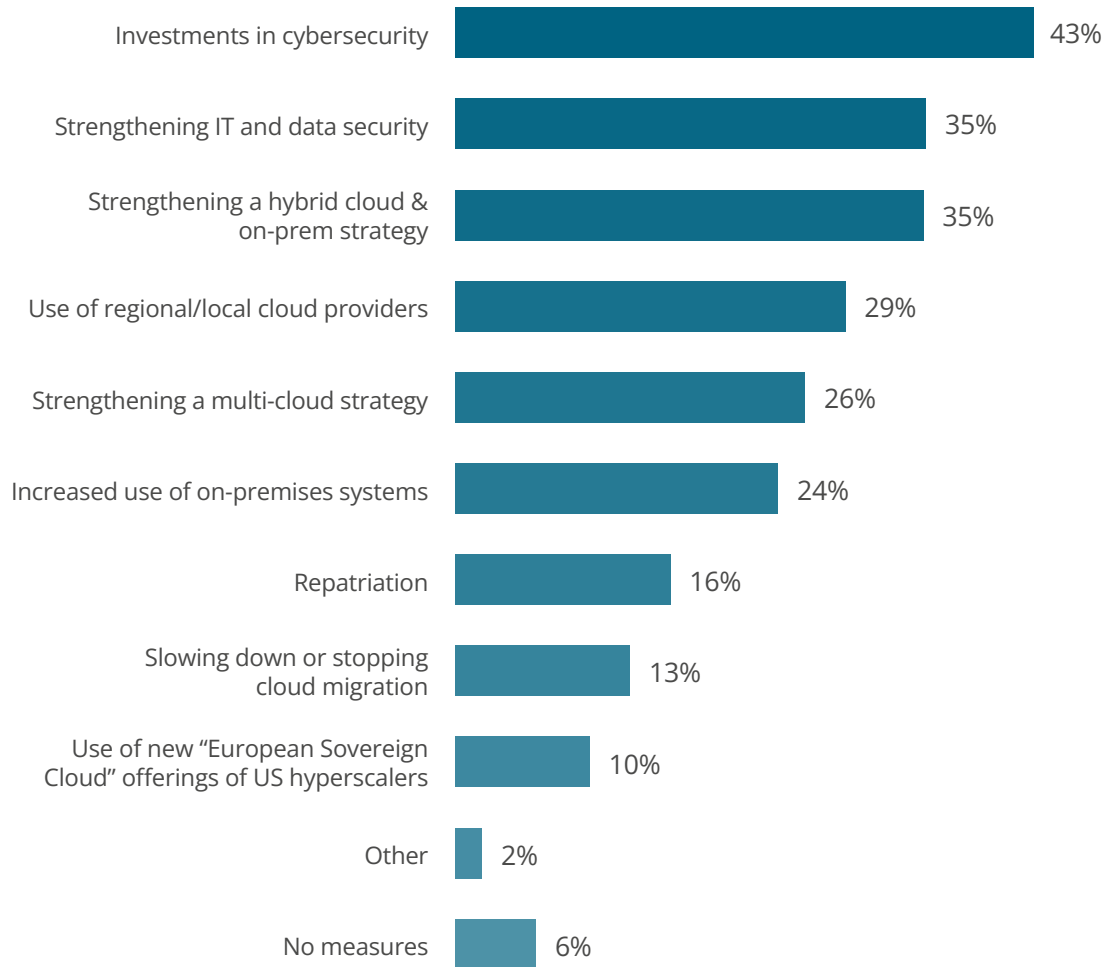


Figure 13: What measures are you taking or planning to take to strengthen your data sovereignty?
(n=304)

Viewpoint



Organizations are addressing data sovereignty mainly through two levers: stronger security investment and pragmatic adjustments to cloud and infrastructure strategy. The top measure is investment in cybersecurity (43%), followed by efforts to strengthen IT and data security (35%). This is especially relevant in regulated industries, where sovereignty goals depend on demonstrable control over access, protection, monitoring, and incident response.

Sovereignty concerns are also reshaping cloud architecture. Many organizations are reinforcing hybrid cloud and on-premises strategies (35%), suggesting a differentiated operating model rather than a full "cloud reversal". Multi-cloud is another key pattern (26%), used to reduce concentration risk, improve resilience, and preserve leverage by keeping workloads portable where feasible.

Provider choice becomes a sovereignty instrument as well: 29% look to regional or local cloud providers, reflecting the desire for clearer jurisdictional alignment and more transparent governance. Interest in "European Sovereign Cloud" offerings by US hyperscalers exists (10%), but the modest share indicates ongoing questions around verifiable control and contractual enforceability. Repatriation (16%) and slower cloud migration (13%) signal selective recalibration. Overall, sovereignty is increasingly treated as a risk-and-control agenda implemented via security, architecture, and provider governance, not as a standalone compliance project.

Trend for On-Premises Systems and Repatriation Continuous

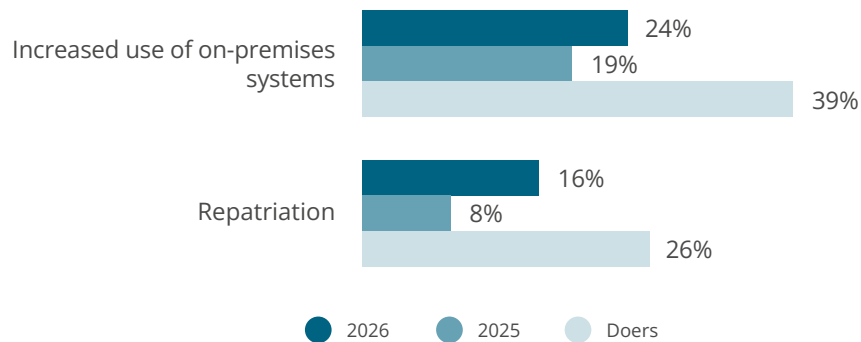
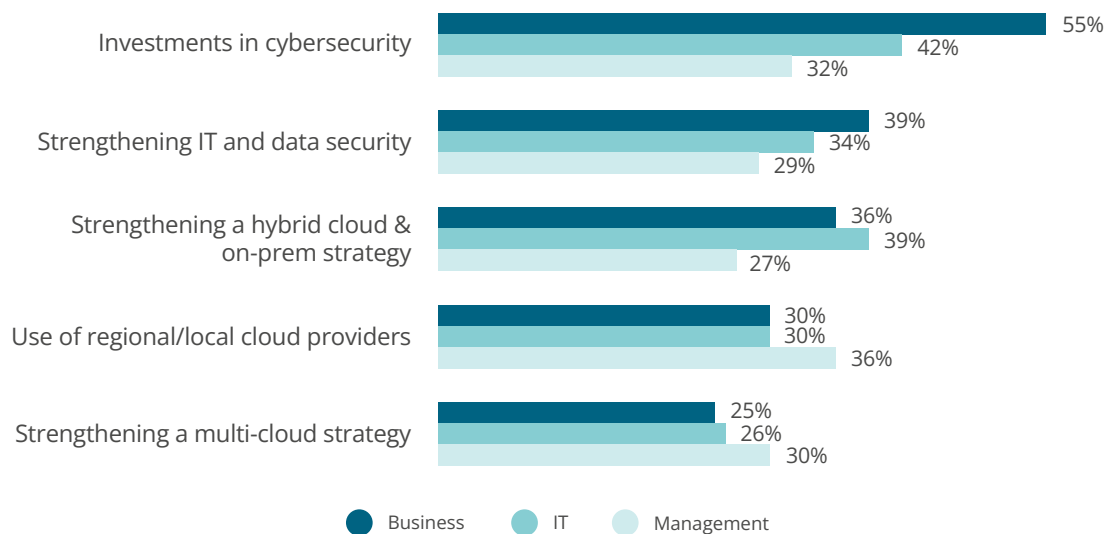


Figure 14: What measures are you taking or planning to take to strengthen your data sovereignty? By role (n=251)

Figure 15: What measures are you taking or planning to take to strengthen your data sovereignty? (n₂₀₂₆=304 | n₂₀₂₅=277 | n_{Doers}=289)

Viewpoint



A role-based view indicates that business respondents are highly focused on security measures: 55% of business users cite investments in cybersecurity as a measure, compared to 32% in management and 42% in IT. IT respondents more often emphasize architectural choices such as hybrid strategies (39%), while management is more focused on regional or local providers (36%).

The role split is healthy when it leads to a coherent program. It becomes a risk when security, architecture, and provider strategy are treated as separate conversations rather than as one sovereignty roadmap.

The data also shows a continued trend toward on-premises and repatriation (the migration from cloud workloads back to on-premises systems): the use of on-premises increased from 19% in 2025 to 24% in 2026, and repatriation doubled from 8% to 16%.

Regulated industries are particularly active in this area, with 33% increasing on-premises use compared to 21% in less heavily regulated industries.

“Doers” stand out even more and are worth highlighting explicitly: Among organizations with dedicated budgets, 39% use or plan to use on-premises technology (vs. 24% overall) and 39% utilize regional providers. “Doers” also apply architectural measures significantly more than others: 52% by strengthening a hybrid architecture (vs. 35% overall) and 45% by strengthening a multi-cloud strategy (vs. 26% overall).

Sovereignty does not automatically mean “no cloud.” It means more deliberate choices about where data is being stored and which providers to trust with that data, clearer boundaries, and the ability to move workloads when risk or dependency requires it.

Data Sovereignty Is No Barrier to Innovation

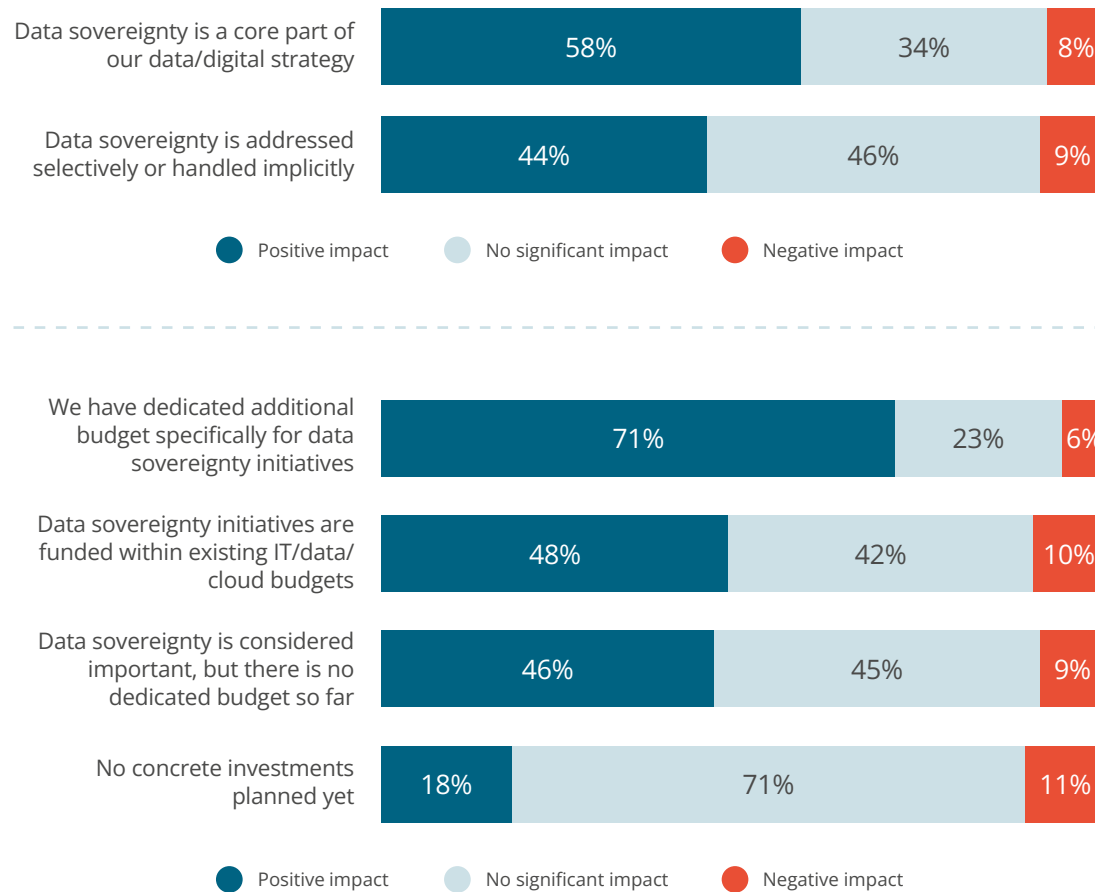


Figure 16: How do you assess the overall impact of data sovereignty initiatives on your company's innovation capabilities? By approach (n=258)

Figure 17: How do you assess the overall impact of data sovereignty initiatives on your company's innovation capabilities? By funding mode (n=286)

Viewpoint



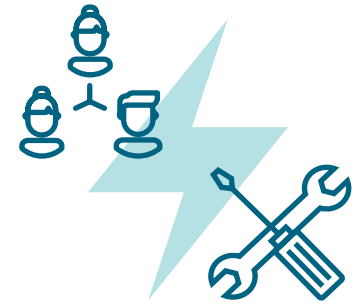
A common fear is that compliance and governance investments, such as in sovereignty, slow down innovation but the survey results suggest the opposite is often true. 46% report a positive impact of sovereignty initiatives on innovation, 45% see no impact, and only 9% report a negative impact.

The effect is stronger among those who act strategically. 58% of organizations that have anchored sovereignty in strategy report a positive impact. Among those with dedicated budgets, 71% report a positive impact.

Sovereignty can enable innovation when it reduces friction and uncertainty. Clear controls, governance patterns, and architectural boundaries can shorten approval cycles and make experimentation safer to scale.

Survey Results

Challenges: People Issues Continue – While Technical Hurdles Surge in 2026



The "People Factor" Remains the Biggest Challenge to Building Sovereign Architectures. Technical Hurdles Emerges as a Major Challenge in 2026

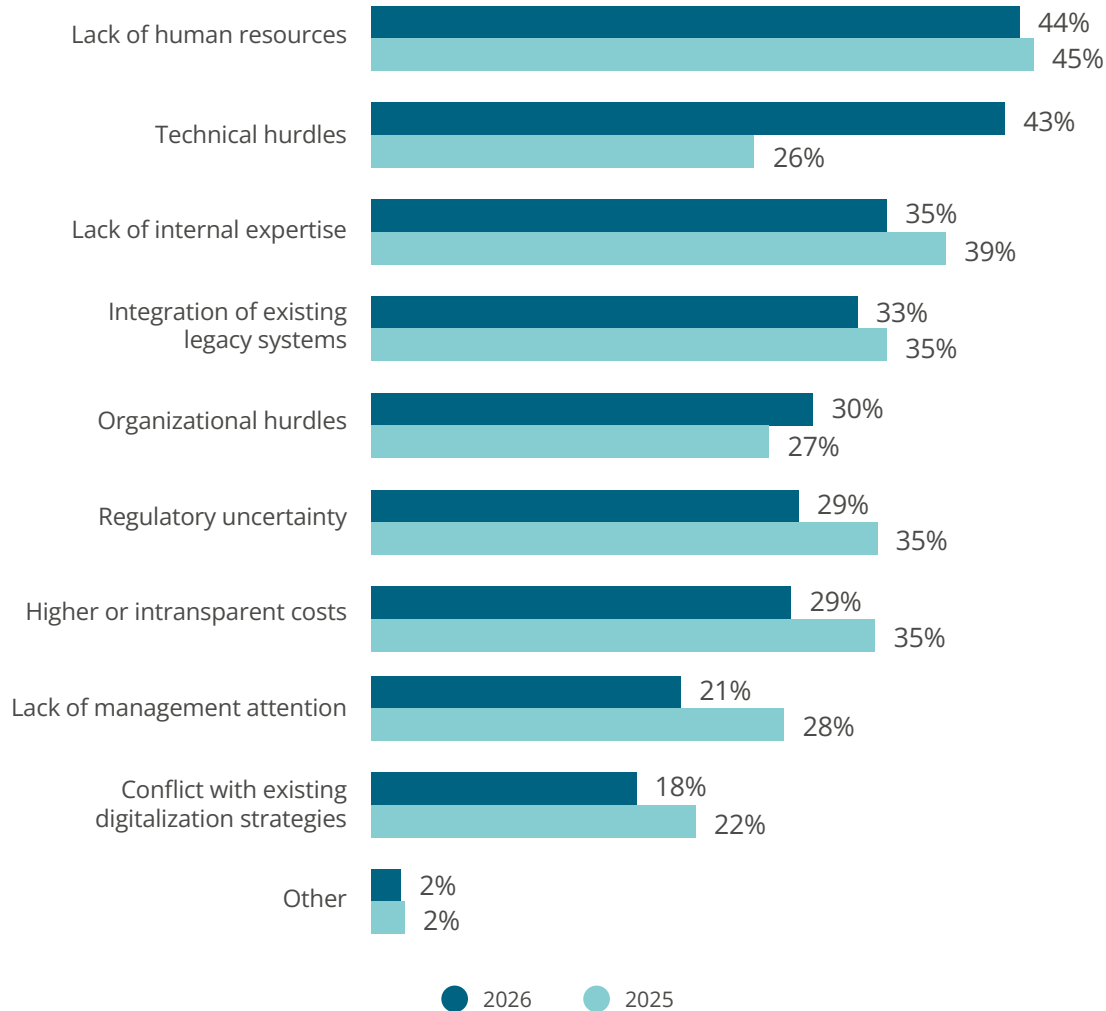


Figure 18: What challenges do you see in implementing data sovereignty in your company?
(n₂₀₂₆=315 / n₂₀₂₅=288)

Viewpoint



Human and organizational constraints remain the strongest barriers. A lack of human resources is cited by 44% and missing internal expertise by more than a third. Organizational challenges are an issue for 30%.

A major change in 2026 has been the sharp rise of technical hurdles as a challenge, increasing from 26% to 43%. Legacy integration is a prominent example, cited by roughly one third of organizations. Interestingly, regulated industries report fewer technical hurdles (30%), which may reflect earlier investments and accumulated experience in building compliant architectures.

A closer look at investment behavior reinforces this execution reality check: for organizations actively investing in sovereign architectures – whether through dedicated budgets or existing funding lines – technical hurdles emerge as the leading challenge. Only among non-investors do resource constraints, skills gaps, and limited management support rank ahead of technical barriers.

Technical hurdles arise when organizations move from “policy talk” to “architecture build”. Once sovereignty becomes real work, legacy reality, integration complexity, and platform constraints become unavoidable.

Recommendations





1 Anchor sovereignty in business and data strategy and establish it as an owned, funded program.

Treating sovereignty as a principle is not enough. The survey shows a persistent gap between stated importance and actual investment, with 40% of organizations not investing at all and only 10% working with a dedicated budget. To close this gap, organizations should define sovereignty as a program with clear scope, ownership, and measurable outcomes, and make the funding model explicit. Whether funding is provided through a dedicated budget or embedded in existing initiatives, it should be transparent, traceable, and linked to concrete results rather than absorbed into unrelated projects.

2 Build a three-pillar roadmap covering strategic alignment, governance and security controls, and technical architecture.

The maturity data suggests that many organizations are progressing unevenly across these pillars, with governance and architecture often lagging behind strategic intent. To address this, the roadmap should be structured explicitly around three dimensions: (a) strategic alignment, (b) governance and security controls, and (c) technical architecture patterns. For each pillar, organizations should define what “well-defined” means in their own context and track progress against that target. This includes clarifying decision rights and escalation paths, standardizing control requirements for data storage and processing, data sharing, and AI use, and defining reusable architecture and security patterns that make controls consistently implementable rather than reinventing them in every project.

3 Use dependency and resilience risk as design inputs, not late-stage concerns.

Concerns about dependence on public cloud providers have grown in the last year, rising from 40% to 46%, while political and cybersecurity considerations have also become more prominent. These risks should be translated into concrete design decisions early on, including portability requirements, exit options, encryption and key management models, workload placement rules, and supplier risk controls. Sovereignty does not mean avoiding cloud by default, but making deliberate decisions about where data and workloads reside, which providers are trusted for which use cases, and how dependencies can be reduced when risk exposure becomes too high. Dependency management should therefore not be treated as a procurement issue alone, but as a core architectural and strategic concern.



4 Treat AI and core-process data as the operational test for sovereignty.

With 62% of respondents citing the growing use of data and AI in core business processes as a key driver of sovereignty, requirements need to be designed with AI-enabled operations in mind from the outset. This means clearly defining which data can be used for which AI-supported decisions, what degree of auditability is required, how data and model lineage are tracked, and how access is controlled across environments. Sovereignty becomes truly operational when AI moves beyond experimentation and into production-critical workflows, where control, traceability, and trust are no longer optional.

5 Reduce people bottlenecks and repeated implementation effort through standardization and enablement.

The leading barriers to stronger data sovereignty remain human resource constraints, skills gaps, and organizational challenges, while technical hurdles such as legacy integration have risen sharply as organizations move from policy discussions into implementation. Programs that rely heavily on a small number of scarce specialists will not scale. Organizations should therefore invest in reusable patterns, templates, reference architectures, and self-service guardrails that allow teams to deliver compliant and sovereign solutions with less need for constant expert intervention. Practical measures include providing “golden paths” for common use cases, offering targeted training for architecture, governance, and security roles, and establishing a small enablement team that supports product and delivery teams throughout implementation instead of reviewing everything at the end.

6 Make sovereignty an innovation enabler by design.

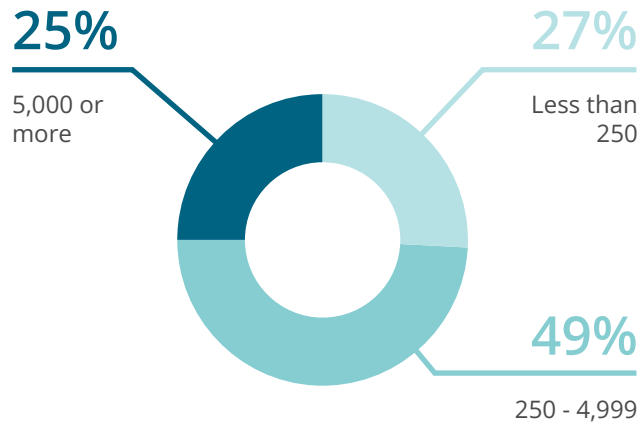
Nearly half of organizations report that sovereignty initiatives have had a positive effect on innovation, and the impact is even stronger among organizations that are actively investing. This should be treated as an explicit design objective: sovereignty should reduce uncertainty, improve trust, and accelerate decision-making rather than create additional friction. Clear governance patterns, reusable controls, and well-defined architectural boundaries can make experimentation safer and scaling easier. If sovereignty creates friction in delivery, organizations should improve automation, clarify implementation patterns, and embed controls earlier in delivery workflows.

Methodology

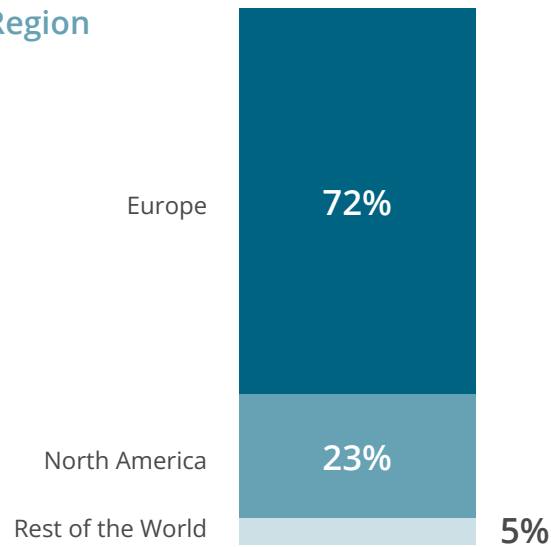


Demographics

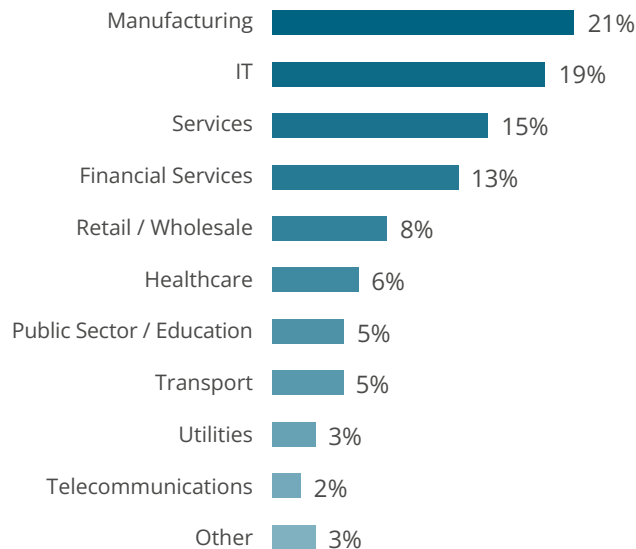
Number of Employees



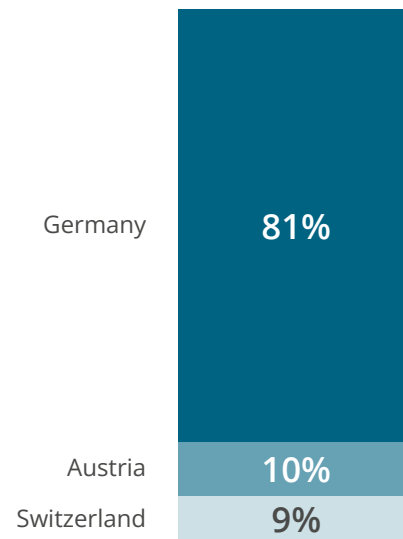
Region



Industry



DACH Countries



Information on the Survey



This worldwide study is based on a quantitative online survey conducted in February and March 2026. BARC promoted the survey within the BARC panel, on websites and via newsletter distribution lists. The objective was to understand the current relevance, strategic importance and practical implementation of data sovereignty in organizations.

After data cleansing, a total of 320 responses remained for analysis. Respondents came from a wide range of industries, company sizes, roles and regions, providing a globally distributed sample.

BARC used a structured questionnaire to capture expertise and practical experience across all three dimensions of the study: reality, relevance, and roadmap. Due to rounding, percentage totals in the figures may not add up to exactly 100. The "I don't know" response option is not included in the sample size shown below each figure and is not displayed in the charts.

About BARC



BARC is the leading analyst firm for data & analytics, AI, corporate performance management (CPM), and ESG with a reputation for unbiased and trusted advice. Our expert analysts deliver a wide range of research, events, and consulting services for the data & analytics community. Our innovative research evaluates software, vendors, and service providers rigorously and highlights market trends, delivering insights that enable our customers to innovate with data, analytics, and AI. BARC's 25 years of experience with data strategy & culture, data architecture, organization, and software selection helps clients transform into truly data-driven organizations.

Research

BARC user surveys, software evaluations, and analyst advisory services along with expert driven content such as research notes, trend analysis, and blogs give organizations the confidence to make the right decisions. Our independent research gets to the heart of market developments, evaluates software, vendors, and service providers thoroughly and gives valuable ideas on how to turn data, analytics, and AI into added value and successfully transform businesses.

Consulting

The BARC consulting practice is entirely focused on translating companies' requirements into future-proof decisions. The holistic advice we provide helps companies successfully implement their data & analytics strategy and culture as well as their architecture and technology. BARC's

research and experience-founded expert input sets organizations on the road to the successful use of data & analytics, from strategy to optimized data-driven business processes.

Events

At BARC events, leading minds and industry experts come together to share insights and drive innovation. Our conferences, roundtables, and online webinars attract over 10,000 participants annually, offering a unique blend of information, inspiration, and interactivity. These events provide a platform to exchange ideas with peers, explore emerging trends, and gain expert perspectives on market developments. By engaging with thought leaders and industry practitioners, participants discover actionable strategies to enhance their business and stay ahead in the evolving world of data & analytics.

Germany

BARC GmbH
Berliner Platz 7
D-97080 Würzburg

info@barc.de
+49 931 880 6510

Austria

BARC GmbH
Hirschstettner Straße 19 / 1 / IS314
A-1220 Wien

info@barc.at
+43 660 6366870

Switzerland

BARC Switzerland GmbH
Buchhaldenstrasse 7
CH-5442 Fislisbach

info@barc.ch
+41 76 340 35 16

USA

BARC US
13463 Falls Drive
Broomfield, CO 80020

info@barc.com
+1 720-381-4988

www.barc.com

BARC

Sponsor Profiles



Actian

Actian empowers enterprises to confidently manage and govern data at scale. Actian data management and data intelligence solutions help streamline complex data environments and accelerate the delivery of AI-ready data. Designed to be flexible, Actian solutions integrate seamlessly and perform reliably across on-premises, cloud, and hybrid environments. Learn more about Actian, the data and AI division of **HCLSoftware**, at actian.com.



ACTIAN™
a division of HCLSoftware

Contact

USA Headquarters

2600 Great America Way
Suite 401
Santa Clara, CA 95054

+1.650.587.5500

actian.com

Office Germany

Entwicklungszentrum Halenreihe 40
22359 Hamburg, Germany

Phone: +49 40 60990-0

Fax: +49 40 60990-113

Exasol

The **Exasol** Analytics Engine is purpose-built to handle the most demanding data workloads at an unmatched price/performance ratio. Trusted globally, it delivers near real-time insights, advanced AI capabilities, and self-tuning functionality – enabling faster, smarter business decisions. Whether used as a standalone data warehouse, analytics accelerator, or AI/ML model enabler, Exasol ensures reliable, high-performance analytics across on-premises and hybrid environments.



Contact

exasol.com



STACKIT

STACKIT is the cloud provider of Schwarz Digits (Schwarz Group). On its way to becoming the first European hyper-scaler, STACKIT offers businesses and partners fully sovereign cloud solutions with the highest security standards. From IaaS to AI platforms: The Neckarsulm-based team provides holistic support for digital transformation, paving the way for an independent Europe.



Contact

Office Germany

Schwarz Digits Cloud GmbH & Co. KG
Stiftsbergstr. 1
74172 Neckarsulm
Germany
+49 7132 30474747
info@digits.schwarz

stackit.com
schwarz-digits.de

T-Systems

Company overview

T-Systems, a Deutsche Telekom subsidiary, is a leading European IT services provider with 26,000+ professionals across 26 countries, 2,500+ AI and data experts supported by Detecon consulting, ~10,000 NVIDIA GPUs on sovereign infrastructure, and over a decade of enterprise cloud operations.

Why T-Systems

- Multi-cloud by design, sovereign by default
- A decade of SLA-driven managed cloud operations
- Full-stack infrastructure for AI outcomes—one partner from token to outcome

Strategy and portfolio

Pioneer in European data spaces

T-Systems is a founding contributor to key European data space initiatives, including Catena-X, Manufacturing-X, and Factory-X —the de facto standards for decentralized data architectures in Europe. The Data Intelligence Hub enables sovereign, federated data exchange at ecosystem scale.

AI and data platform

T-Systems' AI and data strategy is built on five pillars:

- Europe's AI Factory: A sovereign token economy
- Agentic enterprise: Agent orchestration at scale
- Data activation: Enterprise data made agent-ready
- Sovereign by design: Compliance as a moat
- Vertical depth: Domain-specific AI

Key capabilities include AI Foundation Services with 30+ models, unified gateway access, and three-tier sovereignty; Agentic AI Platform with MCP/A2A orchestration, Cedar policy engine, and SPIFFE identity; SmartChat and AI Engineer as RAG-grounded assistants; and an Enterprise Governance Layer aligned with the EU AI Act, BSI C5, DSGVO, 7-layer security, and audit trails.

Autonomous execution with guardrails: Agentic AI

The Agentic AI Platform covers the full lifecycle: readiness assessment (APEX), multi-agent design, MCP/A2A orchestration, Cedar-based policy enforcement, and 24/7 managed operations. Domain agents address manufacturing quality intelligence (30–50% faster defect detection), supply chain risk, clinical documentation, and public sector case handling (50–70% faster) — all in sovereign environments with human-in-the-loop controls.

Sovereign infrastructure

T-Systems' sovereign infrastructure includes:

- T Cloud Public: A sovereign public cloud with EU data residency and no non-EU control-plane dependency
- Industrial AI Cloud: For production-scale data sovereignty with approximately 10,000 NVIDIA GPUs at OTC Biere/Magdeburg for real-time AI, predictive maintenance, and digital twins
- Governed data fabric: A sovereign data platform with IDSA/ Gaia-X-aligned federation for lineage, policy, and federated sharing
- LLM serving without black-box exposure: A Sovereign GenAI stack for isolated LLM hosting and inference from Anthropic, Mistral, and Meta, with no data exposed to external APIs

Professional services: Plan — Build — Run

The services span AI advisory (AI strategy, EU AI Act and agentic readiness), implementation of agentic workflows, RAG, and data platforms; and managed services for 24/7 AI operations, MLOps, and compliance monitoring, backed by a zero-outage commitment. Priority sectors include public, healthcare, defense, automotive, energy, and financial services.

“Organizations that control their data architecture, govern their AI operations, and shape digital ecosystems like Catena-X and Manufacturing-X will define the next era of digital leadership in Europe.”



Sven Löffler

Head of Global Go-to-Market,
AI & Data – T-Systems International

Strategic technology partnerships: NVIDIA | Anthropic | AWS | Mistral | Google Cloud | IBM | Microsoft | SAP



Contact

Office Germany

T-Systems International GmbH 00800 33 090300
Friedrich-Ebert-Allee 140
53113 Bonn
Germany

www.t-systems.com/contact
info@t-systems.com

Collaboration Partner



Big Data & AI World Frankfurt

Big Data & AI World Frankfurt is a leading event for data, analytics, and AI professionals across the DACH region, bringing together industry experts and solution providers to explore the practical implementation of data-driven strategies and artificial intelligence.

It addresses key priorities such as data management, AI adoption, and the scaling of data infrastructures. Through expert-led sessions, panel discussions, and real-world case studies, attendees gain insight into how organisations apply advanced analytics and AI technologies in practice – from initial use cases through to enterprise-wide deployment.

A strong emphasis is placed on data governance, regulatory compliance, and the operationalisation of AI within existing systems. The programme reflects current market priorities,

including the growing importance of explainable, compliant, and scalable AI in line with European regulatory frameworks, alongside the need to ensure transparency, trust, and long-term sustainability.

In addition to the conference programme, attendees can engage directly with solution providers showcasing platforms and services spanning data architecture, integration, governance, analytics, and AI. This provides a practical view of how organisations are addressing critical issues such as data quality, silos, skills shortages, and increasing infrastructure demands to enable real-world application.

The event also acts as a hub for knowledge exchange, connecting data leaders, IT decision-makers, solution providers, and practitioners tackling similar priorities across industries. It

enables peer-to-peer learning, fosters collaboration, and supports the sharing of best practices and proven approaches.

As part of Tech Show Frankfurt, it sits within a wider platform that connects data, cloud, cybersecurity, and data centre communities – bringing together the entire technology ecosystem and offering a comprehensive, end-to-end perspective on modern digital infrastructure.

The next edition will take place on 19-20 May 2027 at Messe Frankfurt in Hall 3 – save the date.

Contact

Messe Frankfurt

Ludwig-Erhard-Anlage 1
60327 Frankfurt am Main
Germany

techshowfrankfurt.de/barc-2027



**BIG DATA
& AI WORLD**

BARC

6 - 7 May 2026 Messe Frankfurt
www.techshowfrankfurt.de

BARC

