accenture

Sovereign Cloud Comes of Age in Europe

How to take back control of data and stay compliant in the cloud

What's happening?

Digital sovereignty is the idea that nation states should be able to exert control over digital businesses and data within their borders. It's gaining significant traction in recent years, driven by shifts in global geopolitics, supply shocks and the need to protect personal data and country or organizations' strategic data.

Why does it matter?

Already, about seven in every 10 countries now have legislation regulating data privacy or digital sovereignty. This is adding complexity and cost for global businesses that operate in the cloud.

What's the solution?

A range of sovereign cloud solutions is emerging, particularly in Europe, which has become the global center of digital sovereignty. Although currently small, this market has the potential to grow rapidly in the coming years.

Where's the value?

Our survey of European companies confirms sovereign cloud can provide a range of enterprise benefits, including greater cloud agility and control of data—also with respect to AI (artificial intelligence) implementation—as well as enhanced resiliency, regulatory compliance and reputation.

What are the challenges?

Digital sovereignty is complex because the politics are moving faster than usual on this topic and the technology is adapting. The emerging sovereign cloud market is cluttered, noisy and fast-moving. And business leaders must recognize there's no silver bullet that will solve all their digital sovereignty needs.

How to respond?

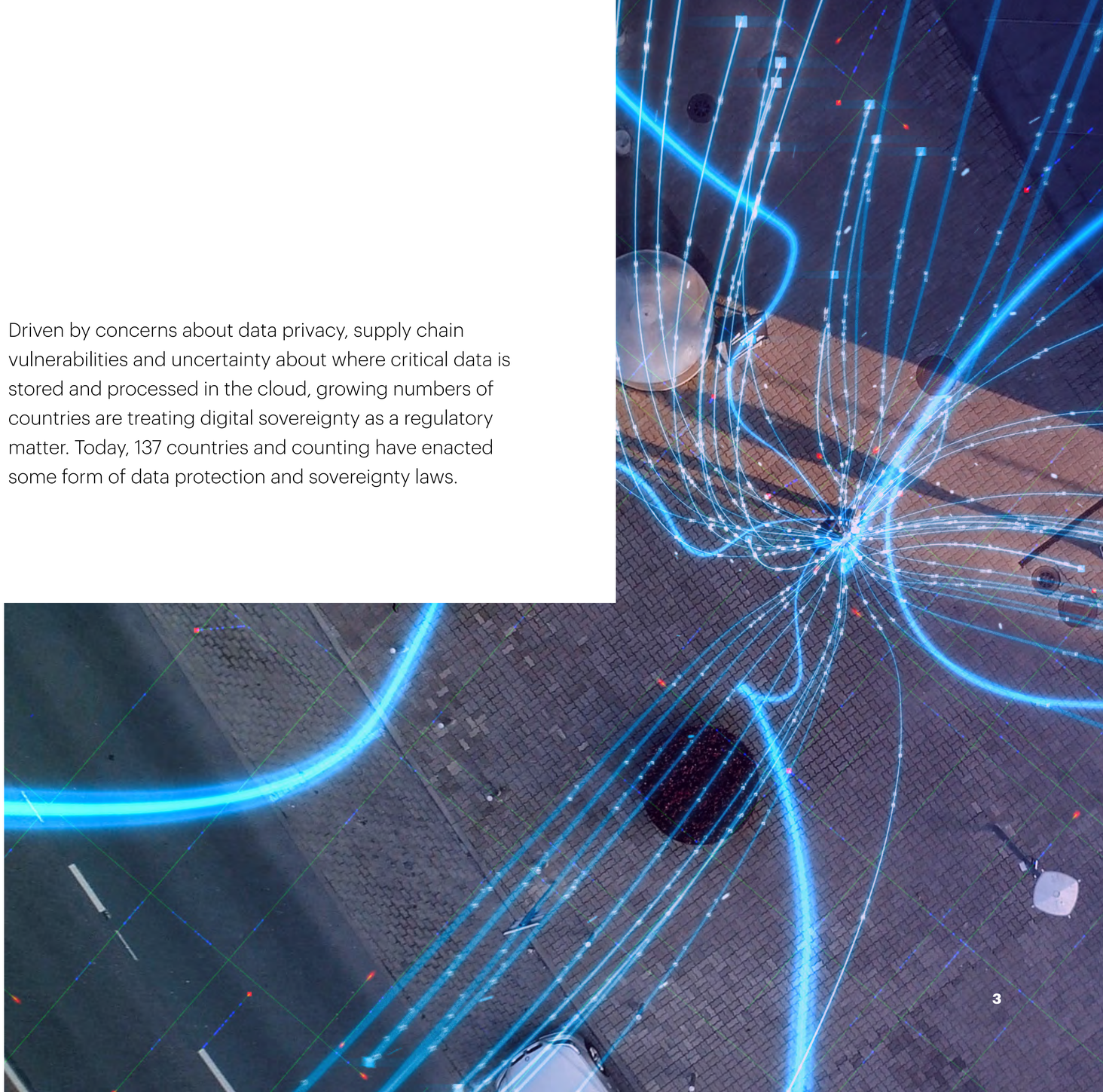
We believe there are several key trends to pay close attention to—including the emergence of local/global cloud vendor partnerships and developing sovereign cloud ecosystems. We also believe sovereign cloud is a transformation, not a quick fix.

Digital sovereignty goes viral

In a time of unprecedented disruption, fast-changing technology and evolving data privacy regulations, digital sovereignty is a critical hurdle to be cleared on the road to business value. That's because cloud, data and AI, together, help power the digital core that has become a primary source of competitive advantage for companies. Top performers are relying on a strong digital core to drive a new imperative: Total Enterprise Reinvention. It's a strategy that aims to set a new performance frontier for companies and the industries where they operate. Control and protection of data assets are essential to utilizing data's full power for enterprise reinvention.

> Digital sovereignty—the idea that nation states should be able to exert control over digital businesses and data within their borders—has become a hot-button topic around the world.

Driven by concerns about data privacy, supply chain vulnerabilities and uncertainty about where critical data is stored and processed in the cloud, growing numbers of countries are treating digital sovereignty as a regulatory matter. Today, 137 countries and counting have enacted some form of data protection and sovereignty laws.



But it's not just governments that are concerned about digital sovereignty. Businesses, too, have been looking deeper at where their critical data sources in the cloud actually reside, and what control they can exert over them. This has become all the more important given the supply vulnerabilities exposed by the COVID-19 pandemic and again during the Russia-Ukraine war.

Europe, in particular, has been driving the digital sovereignty agenda, with governments, businesses and regulators all coming together to develop a comprehensive regulatory framework. This is having a growing impact on global companies. Our research finds 84% of surveyed organizations say European Union regulations have had a moderate-to-large impact on their data handling. The implications for businesses are far-reaching, affecting their ability to thrive in the cloud.

> Our recent survey of global leaders found that "security and compliance risks" was tied as a top barrier to achieving expected cloud value, with 41% citing it as a top 3 concern.

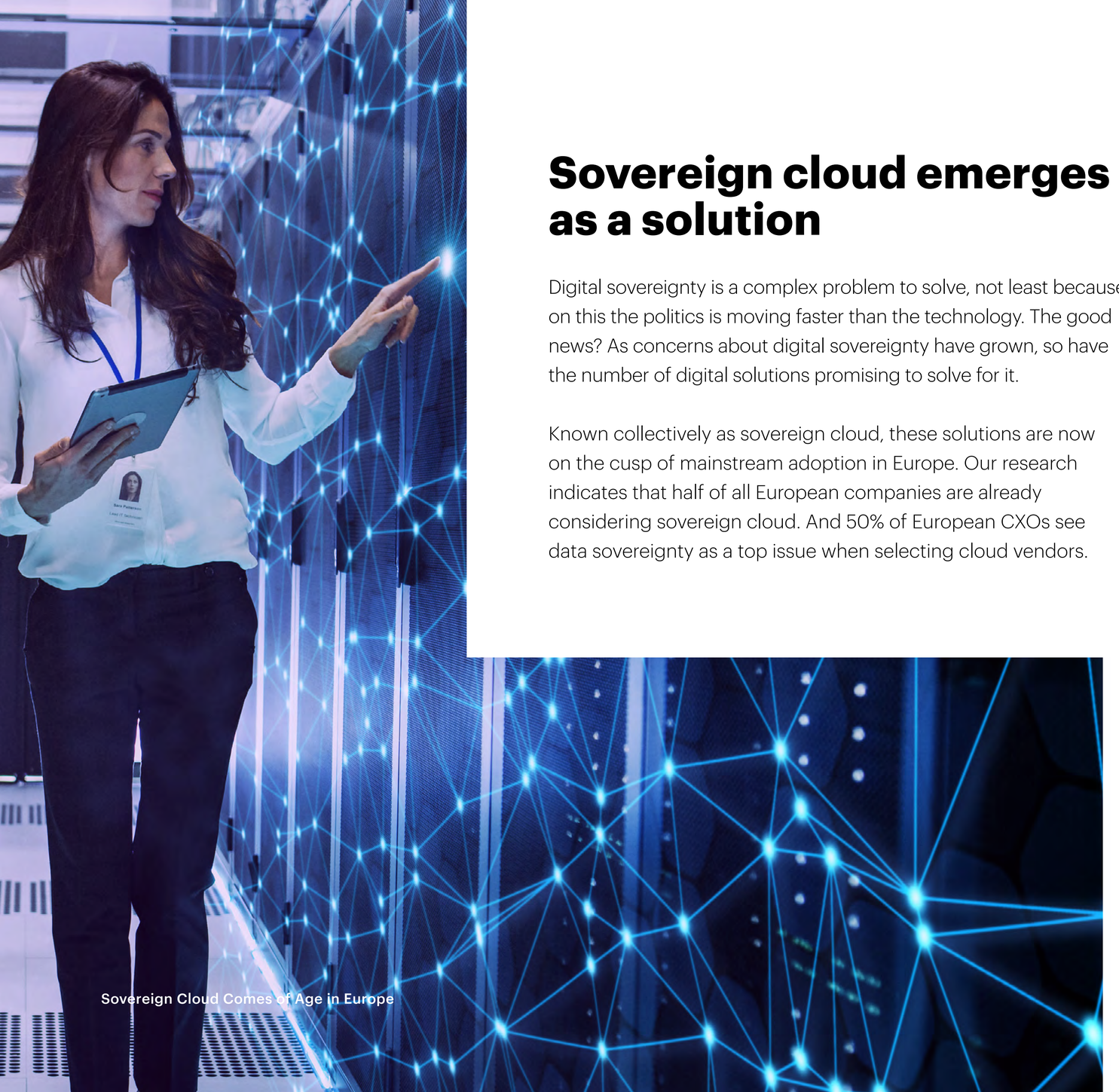
The key message? More and more companies, especially those operating in Europe and/or sensitive industries, are being exposed to digital sovereignty risks they may not be prepared to handle. These companies must now take action to maintain physical and digital control over strategic assets including data, algorithms and software, without affecting their abilities to innovate and deliver for customers. The big question is how companies can navigate this highly charged environment.

Europe's evolving sovereignty strategy

The European Union's data sovereignty strategy is underpinned by numerous regulations and proposals for governing who can use and access certain data, and for which purposes, across various sectors. These include the Data Governance Act, Data Act, and European Health Data Space, among others.

Most recently, the European Council formally adopted the Digital Service Act (DSA), which looks to protect the digital space against the spread of illegal content and ensure the protection of users' fundamental rights. The DSA defines clear responsibilities and accountability for providers of intermediary services, such as social media, online marketplaces, very large online platforms (VLOPs) and very large online search engines (VLOSEs).

Its rules are designed asymmetrically, which means that larger intermediary services with significant societal impact (VLOPs and VLOSEs) are subject to stricter requirements. Each EU Member State will determine its own penalties for DSA infringements under its own competence.



Sovereign cloud emerges as a solution

Digital sovereignty is a complex problem to solve, not least because on this the politics is moving faster than the technology. The good news? As concerns about digital sovereignty have grown, so have the number of digital solutions promising to solve for it.

Known collectively as sovereign cloud, these solutions are now on the cusp of mainstream adoption in Europe. Our research indicates that half of all European companies are already considering sovereign cloud. And 50% of European CXOs see data sovereignty as a top issue when selecting cloud vendors.

> Sovereign cloud is an umbrella term for a range of solutions that enable organizations to take control of the location, access and processing of their data in a cloud environment.

These solutions look to address two principal concerns:

- **Cloud's overlapping legal jurisdictions.** Most cloud hyperscalers are incorporated in the United States and subject to U.S. law. This can create conflicts when it comes to data protection. For example, the 2018 CLOUD Act, which gives certain rights to U.S. law enforcement to access data even if stored in another country, has given rise to concerns among European governments, enterprises and data subjects about potential violations of General Data Protection Regulation (GDPR).

- **Cloud's boundlessness.** The fact that data in the public cloud can be stored, queried and analyzed across borders means there's a significant risk of companies themselves breaching local or regional data residency and protection laws. This is also true of metadata—data about data—which can often itself contain sensitive information. Examples include email metadata indicating who sent a message, and when.

Bringing sovereign cloud to German healthcare and public sector

In Germany, Google Cloud and T-Systems are partnering to provide scalable sovereign cloud to healthcare and public sector organizations. The solution increases openness and transparency for cloud customers, while access to data and facilities (such as routine maintenance and upgrades) is under the supervision of the vendors.[1]

University Medical Center Mainz has chosen IBM Cloud Satellite to digitize clinical processes while addressing data protection and security. This is enabling it to build hybrid cloud-based solutions such as a messenger system for secure communication among medical staff and a mobile app to manage COVID-19 testing while adhering to Germany's data privacy standards.[2]

A niche market with growing potential

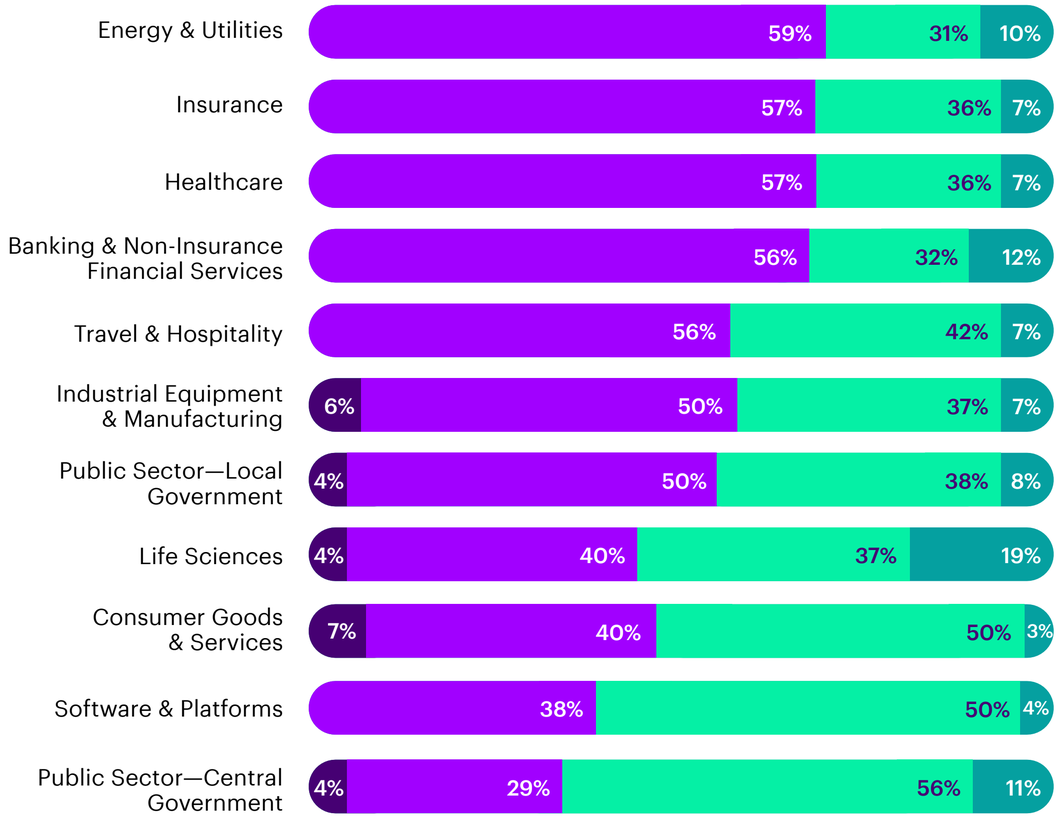
Today, the size of the European sovereign cloud market is still relatively small, especially when compared with the total cloud market in the EU. But it has the potential for rapid expansion, especially given increased regulatory emphasis on data sovereignty and the growing volumes of enterprise data being generated, stored and processed in ever more locations, from public cloud, to edge networks and IoT devices, to metaverse and generative AI.

In fact, our survey finds increasing numbers of European enterprises prioritizing cloud sovereignty over the near term, especially in sectors such as life sciences, consumer goods and public services (see Figure 1). What's more, a huge 89% of enterprises responded that the Russia-Ukraine war has strengthened their focus on sovereign cloud.

- Not a priority for us
- A work in progress
- Not included yet, but planning in next 12 months
- Well-defined

Cloud sovereignty is a "work in progress" for most sectors, led by energy & utilities, insurance, healthcare and others

Figure 1 - Cloud sovereignty strategy by sector



Source: Accenture Sovereign Cloud Survey in Europe, October 2022; N=300

Overall, of those companies who have made or are considering sovereign cloud investments, we found that more than a third (37%) have already invested and nearly half (44%) are planning to do so in the next two years. And almost 60% of surveyed organizations already have or are planning a dedicated CIO team to look at sovereign cloud regulations affecting cloud investments.

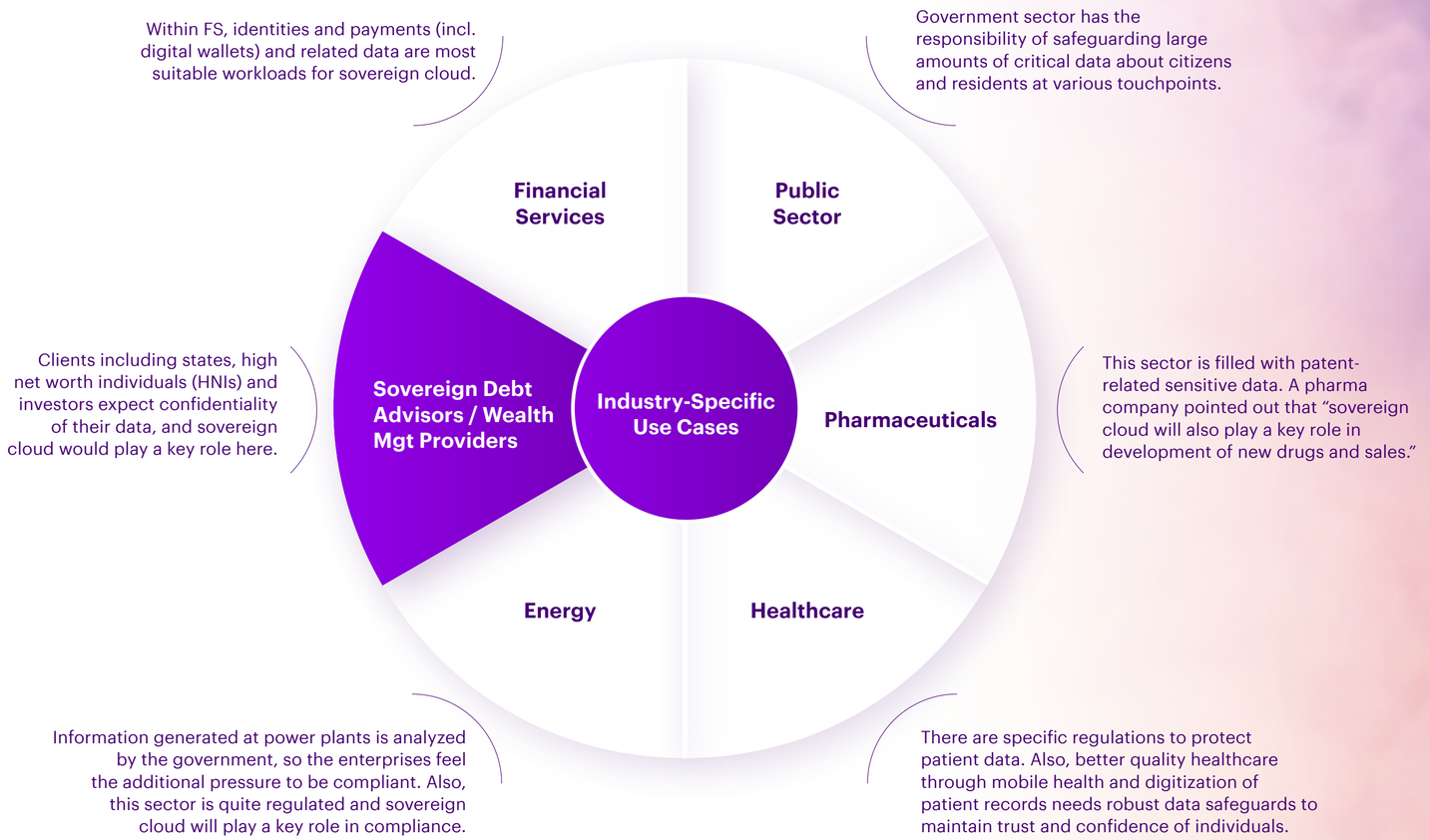
What's more, sovereign cloud could ultimately become the predominant choice for some enterprises. Our research finds that, within companies running pilots today, as much as 20% of workloads are already being moved to sovereign cloud. And more than a third of surveyed companies see the potential for eventually moving between 25% and 75% of data, workloads or assets to sovereign cloud.

Today, the workloads being migrated are mostly those that are business-critical or require more control over residency as a result of regulations. Legal, marketing and sales, and R&D departments have emerged as early buyers of sovereign cloud, but there are numerous other use cases (see Figure 2).

Industry-specific use cases as highlighted by Europe-based executives

Based on our interviews with Europe-based executives, at a cross industry level, legal, marketing and sales (as it has strategic information), and R&D departments are suitable buyers of sovereign cloud.

Figure 2 - Key use case enterprises want to implement with sovereign cloud



Source: 22 in-depth interviews over 2021 and 2022 with European CXOs of mid-sized to large companies

Securing the UK's sensitive data

The UK government, healthcare and defense sectors chose UKCloud as a strategic cloud provider to host sensitive government systems and meet their needs for data residency and data sovereignty. The platform is based solely in the UK and operated 24/7 by UK security-vetted technical personnel. UKCloud's platform has also helped a London research hospital securely analyze COVID-19 data relating to 2.5 million people and enable collaboration between various scientific research groups.[3]

Where's the value?
Compliance, customer-centricity, control

From our in-depth interviews with European executives, we find companies considering sovereign cloud are looking to achieve a range of different enterprise benefits:

Increased control

Responsible organizations expect data to always be used and transferred safely, regardless of regulatory requirements. Enterprises expect sovereign cloud to help them keep control of their data globally, not only across their own international operations but also the wider ecosystem of partners, employees, government and other stakeholders.

Regulatory compliance

Enterprises expect sovereign cloud to support improved data protection and privacy, ensure industry compliance, safeguard intellectual property rights and protect their interests and data in an evolving global information security and regulatory environment.

Reputation

Many enterprises recognize that, by enhancing the protection and transparency of data, sovereign cloud can increase customer trust and drive retention, as well as support an image-building marketing initiative.

Resiliency

From the pandemic to the Russia-Ukraine war, minimizing the impact of external disruption has become a top priority over the past few years. Understanding and controlling data across international operations are central to that objective. This is one reason nationally important industries (defense, government, energy, telecoms, banking and so on) have tended to be the first to consider sovereign cloud.

Supplier integration

Most large enterprises work with numerous suppliers across their business functions, making the integration of data management systems a complex exercise. Our research shows companies expect sovereign cloud to help solve this complexity and create a common data layer that provides a single source of truth across the enterprise.

Cloud agility

Our survey shows enterprises expect to mix and match different cloud providers—including custom sovereign cloud solutions—to meet their compliance requirements and business objectives. They also expect sovereign cloud to streamline their abilities to migrate apps and services to different IT infrastructure providers. As one energy executive explained, "On the operations side, the sovereign cloud is quite excellent on the tool stack."

Smartphone-based research gets a security boost with Fortanix and Google Cloud

In the Netherlands, the University of Groningen is maintaining data sovereignty with Fortanix and Google Cloud Platform (GCP). The institution collects smartphone-based data as part of its research into mental health and brain disease. To protect participant privacy, the data is hosted on GCP using its cloud-native encryption and key management service. To gain more control over encryption keys and protect against government data subpoenas, the institution is also using the Fortanix Data Security Manager platform. This means it can enable/disable access to data from specific instances and locations at the click of a button.[4]

A series of questions yet to answer

Many companies still have unanswered questions about sovereign cloud. Given the relative immaturity of the market, that's inevitable. These companies are seeking clarification about sovereign cloud pricing, its return on investment, its reliability, how to manage it internally, its talent implications and how it compares with hyperscaler solutions—not to mention how it will adapt to a regulatory and geopolitical environment that will inevitably keep evolving in the future.

Figure 3 - **Key questions European enterprises are asking about sovereign cloud**

Responsibility

- How do we define sovereign cloud?
- Who is internally responsible?

Trust

- How foolproof are sovereign cloud solutions?
- Will they ensure 100% compliance, all the time?
- How can we use generative AI responsibly and in compliance with local laws?

Regulations & Geopolitics

- How would GDPR and other regulations evolve? What are individual country specific data policies that keep evolving?
- If some countries take a lenient approach to data protection, would this add to the complexity of non-standardization?

Talent

- How do we find or train resources with specific skill sets and expertise around sovereign technology and regulations?

Pricing and ROI

- Would sovereign cloud be more expensive than public cloud?
- What are the cost implications of moving data across clouds?
- Is there a justifiable ROI for the additional costs and efforts required to implement sovereign cloud?

Vendor Solutions

- How do vendor solutions compare with public cloud solutions?
- Are sovereign cloud offering relevant at a global level?
- What are the cloud provider offerings around isolated in-country platforms with independent authentication, storage and compliance requirements?
- How do they evolve with the evolution of regulations?
- How do they incorporate a new regulation into their solutions and make sure they are always compliant?

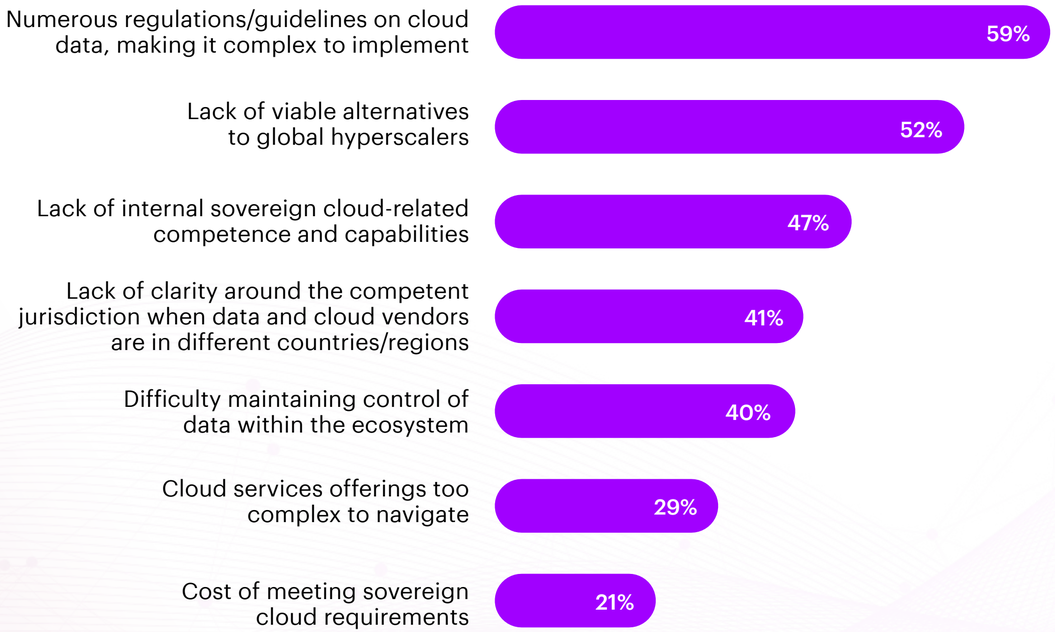
Source: 22 in-depth interviews over 2021 and 2022 with European CXOs of mid-sized to large companies

> Our survey shines a light on some of the challenges companies are facing today.

First and foremost, these challenges relate to the complexities brought on by a multitude of regulations and guidelines (see Figure 4). What's more, because sovereign cloud is a relatively new concept with limited use cases to date, many enterprises are still figuring out how to address their compliance and data protection needs. The expectation of more solutions entering the market is also making it tough for some businesses to make investment decisions.

Most organizations are struggling to navigate around various regulations and compliance related to sovereign cloud

Figure 4 - Survey question: What are the key challenges related to sovereign cloud adoption that your company is facing?



Accenture Europe-based Sovereign Cloud Survey, October 2022; N=300; combination of top 3 ranks by respondents

Given all this complexity and uncertainty, how should companies be approaching their sovereign cloud decisions?

We believe there are several key trends and success factors to consider, such as emerging vendor partnerships, developing ecosystems and transformation best practices.

A partner play, not a solo venture

One of the key trends emerging as the sovereign cloud market matures is the importance of multi-vendor partnerships. In Europe, for instance, some local technology vendors are collaborating with global hyperscalers to allow their customers to benefit from digital sovereignty protections without compromising on best-in-class cloud technologies.

Examples include Thales's partnership with Google, SAP's partnership with Arvato and Microsoft partnership with Telefónica. Similarly, Capgemini and Orange joined forces to create Bleu, a French hyperscale cloud powered by Microsoft Azure to meet the privacy, data sovereignty, governance and transparency requirements of the French government.

Global hyperscalers are themselves also continuing to meet European requirements. In November 2022, AWS announced its "AWS Digital Sovereignty Pledge", its forward-looking and indeed long-standing commitments to continue to make AWS Cloud sovereign-by-design.

By expanding sovereign controls and features in its public cloud offerings, AWS is looking to ensure customers always have full control over the location of their data, verifiable control over data access, the ability to encrypt everything everywhere, and resilience of the cloud, to allow customers around the world to address their digital sovereignty requirements without compromising on the full power of the AWS Cloud.[5]

Microsoft also announced a new set of principles and programs to enable more collaboration with local cloud providers and to serve governments with sovereign solutions powered by confidential computing features developed in collaboration with leading chipset producers.

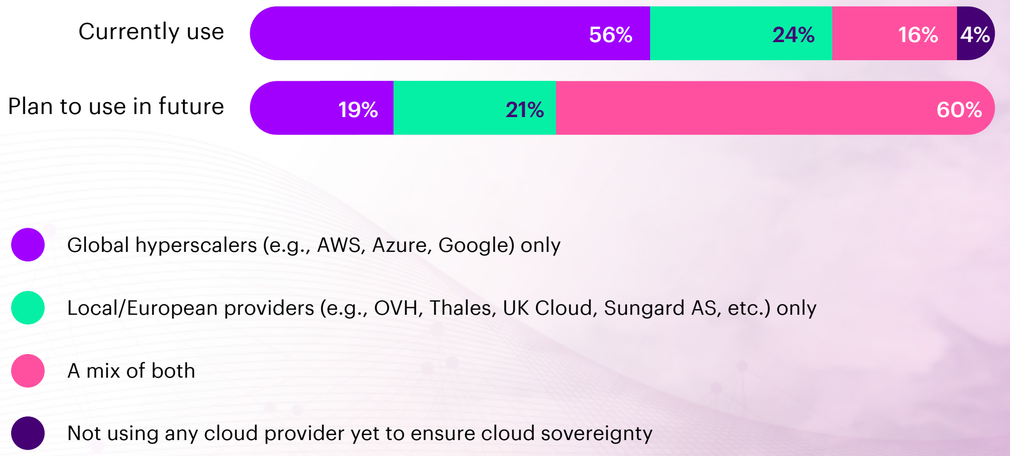
> These principles will guide all aspects of its cloud business, enhance transparency for the public and meet European governments' sovereign needs in partnership with local trusted technology providers.[6]

Similarly, Oracle has launched new sovereign cloud regions for customers across the European Union. These regions further enhance Oracle Cloud Infrastructure's (OCI's) existing capabilities for data residency, security, privacy and compliance, and provide a framework for data and operational sovereignty, including how customer data is stored and accessed, and how government requests for data are handled. The first two Oracle sovereign cloud regions for the EU will be in Germany and Spain, with operations and support restricted to EU residents and specific EU legal entities. The sovereign cloud regions will be logically and physically separate from the existing public OCI Regions in the EU. Currently OCI operates six public OCI Regions located in the EU: Amsterdam, Frankfurt, Paris, Marseille, Milan and Stockholm.

Our survey confirms this trend toward multi-vendor solutions is growing fast. Europe-based enterprise respondents told us they plan to rapidly increase their use of a mix of global and local cloud providers in the future (see Figure 5).

Increasingly, European enterprises plan to use a mix of both local and global cloud providers

Figure 5 - Survey question: Which cloud vendors do your organization currently use or plan to use to ensure cloud sovereignty?



Accenture Europe-based Sovereign Cloud Survey, October 2022; N=300

Combining cloud agility with data security

Leading French healthcare software provider Maincare Solutions selected HPE GreenLake to provide a resilient and agile cloud-based environment for SaaS healthcare solutions while meeting data security requirements. A state-of-the-art data center on French soil ensures compliance with stringent standards and certifications, including ISO27001 and HDS certification, and allows Maincare to provide sovereign cloud services to its customers.[7]

Emerging ecosystems show the way forward

Aside from vendor partnerships, the broader sovereign cloud ecosystem is becoming increasingly important in bringing interested parties together and defining relevant frameworks and standards.

These ecosystems include regional and national policymakers, representatives from regulated sectors and critical industries most likely to be impacted by data sovereignty requirements, and industry alliances, consortiums and associations. Plus, of course, the hyperscalers, potential sovereign cloud providers and other enterprise technology vendors.

Sovereign ecosystem actors in every country

Rules

National Policymakers

- Governments / politics
- Regulatory bodies / authorities
- Digital agenda owners
- Recovery funds stakeholders

Influence

Sovereign Communities

- Gaia-X hubs
- Alliances for Cloud and Edge
- Data spaces
- Lobbying groups

Co-opetition

Sovereign Ecosystem

Demand

Regulated Clients

- Health and public sector agencies
- Energy: critical infrastructures
- Financial services: sensitive data owners
- Products: industrial data owners

Supply

Potential Sovereign Cloud Providers

- Telcos
- Government IT in-house companies
- Large critical infrastructure operators

Technology Vendors

- Hybrid: IBM, Red Hat, VMware, HPE, Dell
- Network & security: Cisco, Fortinet, Palo Alto Networks, Thales
- Data: Informatica, SAS, SAP, Cloudera
- GPU/CPU: Intel, Nvidia, AMD
- Generative AI: Open AI, Silo AI, Cohere, DeepMind

Hyperscalers

- AWS, Google, Microsoft, Oracle

Components

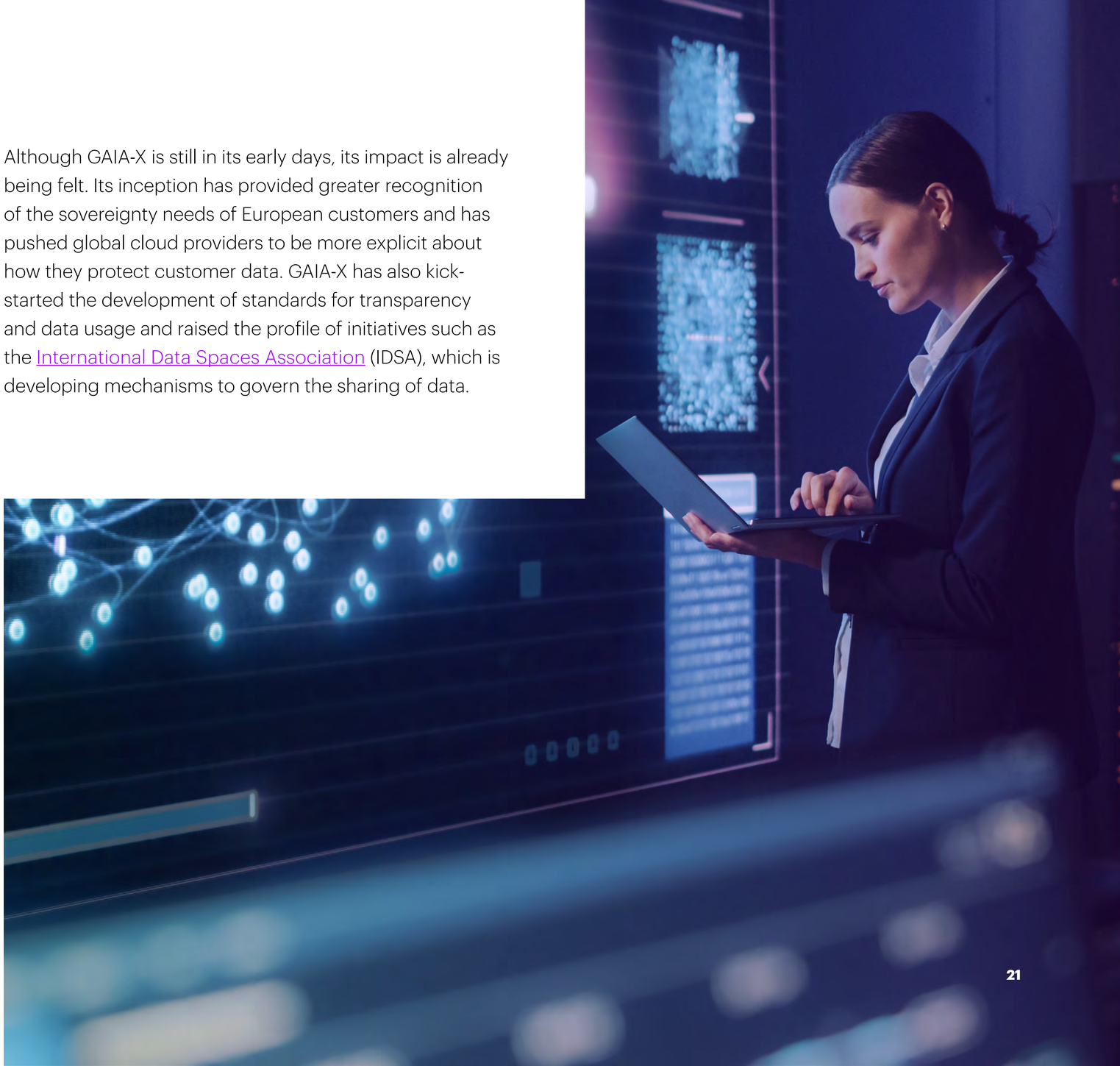
Solutions

Europe's GAIA-X is a good example of the way the market is developing. The initiative, which aims to support the development of a sovereign cloud ecosystem for European countries, companies and citizens, started with just 22 members but has grown to include more than 300 representatives from business, politics and science.[8]

> GAIA-X is developing frameworks and standards to support a secure and trustworthy foundation for a European cloud infrastructure that is technically interoperable and boosts opportunities for collaboration.

And its reach is expanding globally—U.S.-based hyperscalers such as AWS[9] and Microsoft[10] are already exploring how best to support GAIA-X.

Although GAIA-X is still in its early days, its impact is already being felt. Its inception has provided greater recognition of the sovereignty needs of European customers and has pushed global cloud providers to be more explicit about how they protect customer data. GAIA-X has also kick-started the development of standards for transparency and data usage and raised the profile of initiatives such as the International Data Spaces Association (IDSA), which is developing mechanisms to govern the sharing of data.



Banking on sovereign cloud

Spain's CaixaBank SA selected IBM Global Services' IBM Cloud for Financial Services to scale its hybrid cloud adoption while addressing data sovereignty requirements. IBM's multizone region (MZR) enables European companies to deploy mission-critical workloads with high levels of security and compliance. This helps the bank offer its 21 million customers a better user experience while reducing regulatory barriers to modernizing its IT landscape.[11]

A transformation, not a quick fix

Adopting sovereign cloud needs to be considered as a transformation and the technology is only part of the equation. Organizations also need to consider C-suite buy-in and the overall impact on processes, data and people.

It's why we believe the following sovereign cloud best practices are critical:

Strengthen data management

It's essential to be able to distinguish critical and/or sensitive data from other data for the purposes of regulatory compliance, which calls for robust data classification and management. Companies must also understand how data flows within their organizations and conduct a thorough data protection impact assessment (DPIA) before moving to a sovereign cloud.

Enhance control and trust

Establishing the necessary control over data can be a complex process, especially in global companies where data is moving across borders. We find organizations that develop a specialized competency center (either in-house or with partners) to oversee data governance across the enterprise are better able to manage that complexity. Such an approach also helps build trust within the organization and ensures access to the right talent.

Learn from a multi-cloud approach

Companies with mature cloud strategies encompassing multiple vendors and a hybrid cloud approach tend to adopt sovereign cloud earlier and more easily. This makes sense—experience with hybrid and multi-cloud improves a company's ability to test multiple local-global cloud vendor partnerships and choose the combination that best meets its needs.

Select the right vendors

Finding the right cloud partners is especially important in sovereign cloud projects. Not only that, such projects usually also call for a multi-vendor/ecosystem approach, because no single vendor is likely to be able to provide all the services and options required. These partners should be selected carefully, based on their cloud and industry expertise, as well as their knowledge of region-specific regulations.

Cut through the clutter and unlock the power of sovereign cloud

Vulnerabilities exposed by the pandemic, war and economic disruption and generative AI—which have ignited concerns about digital sovereignty—are also driving a larger reinvention imperative for enterprises across the globe. Data and cloud work together in the digital core to drive business agility and resilience as well as breakthrough innovations. With data emerging as a critical national and economic asset, organizations must increasingly consider sovereign cloud a core component of their overall IT strategies.

Cutting through the clutter of the nascent sovereign cloud market is the key to finding value. That means taking a holistic view of data, focusing on priority use cases and workloads, and finding partners with experience in implementing tailored multi-vendor solutions.

Ethical AI and sovereignty need three main components:

- A trusted IT platform that can deliver computing power at scale and completely under your control (Sovereign HPC)
- Full control of data feeding the AI algorithm, such as location, access, permissions and insights
- A trusted and familiar ecosystem of developers who produce, maintain and train the AI/ML (machine learning) model

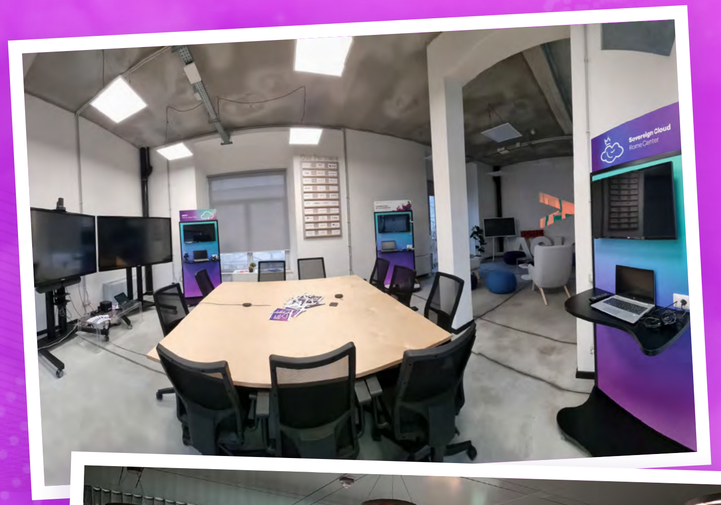
> In this way, organizations can develop a sound sovereign cloud strategy that delivers enhanced transparency and trust, helps them take control of their data, and unlocks new sources of value in the digital realm.

Continue the conversation:
Accenture’s sovereign cloud position and offerings

Come talk to us!

Accenture is one of the first companies to have recognized the importance of the burgeoning sovereign cloud sector. Our dedicated Cloud First Sovereign Practice includes four new sovereign cloud centers in Kronberg, Trondheim, Paris and Rome. Located within Accenture Innovation Hubs, these centers bring Accenture industry, security and technology specialists together with ecosystem partners to accelerate the digitization of business processes and expose new data collaboration opportunities. Accenture’s Cloud Security Center of Excellence also provides leading-edge services in the cloud and security capabilities.

Rome Center



Kronberg Center

Authors

Koenraad Schelfaut

Cloud First Lead, Europe

Koen is a Senior Managing Director and Accenture's Cloud First Lead for Europe. He is also a member of the Accenture European Executive Committee. He has worked extensively with European CEOs from all partners, focusing on joint proactive go-to-market activities and creating relevant industry-specific assets as well as setting up strong multidisciplinary teams in six market units.

Mauro Capo

Sovereign Cloud Lead, Europe

Mauro is a Managing Director in Accenture Technology Cloud First, where he holds a double responsibility as leader for the new Accenture Sovereign Cloud Practice for Europe, and Cloud First for the Health and Public Services market in a geography that covers Italy, Central Europe and Greece. In his industry role, Mauro is in charge of the end-to-end sales and delivery activities for projects on technology infrastructures, applications and data of government agencies, which involve digital core transformation through the use of cloud solutions.

Surya Mukherjee

Research Lead, Europe Technology

Surya Mukherjee is a Senior Principal at Accenture and Head of Technology Research for Europe. He has more than two decades of experience as an advisor to platform providers and their users, and has been quoted in the Wall Street Journal, ZDnet and Computer Weekly. His interest lies in exploring the transformative impact of technologies on industries, companies and brands.

Accenture Research Team

Research Lead - Jai Bagmar

Research team

Chiara Addis, Ajay Garg, Paul Merry

Acknowledgments

Griet Joppen, Guido Greber, Paolo Snidero

References

[1] Joint invest in technology solutions and co-innovation to serve local customer needs (2021)

[2] University Medical Center Mainz Adopts IBM Cloud Satellite to Digitize Its Clinical Processes (2021)

[3] Sovereign Clouds: Partner Perspectives on Safeguarding Critical Customer Data (2022)

[4] University of Groningen achieves European data sovereignty and data compliance with Fortanix External Key Management for Google Cloud Platform (2022)

[5] AWS Digital Sovereignty Pledge: Control without compromise (2022)

[6] Microsoft responds to European Cloud Provider feedback with new programs and principles (2022)

[7] French Healthcare Software Provider, Maincare, Selects HPE GreenLake to Accelerate Deployment of Secure Health Cloud Services (2022)

[8] GAIA-X is developing frameworks and standards (2022)

[9] What's next for Europe's data revolution? AWS joins the GAIA-X initiative (2020)

[10] Microsoft announced as a member of GAIA-X (2020)

[11] CaixaBank boosts digital capabilities with IBM Cloud for Financial Services; Onboards to New IBM Cloud Multizone Region in Spain (2021)

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Technology and Operations services and Accenture Song—all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 738,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities.

Visit us at **www.accenture.com**

About Accenture Research

Accenture Research creates thought leadership about the most pressing business issues organizations face. Combining innovative research techniques, such as data science led analysis, with a deep understanding of industry and technology, our team of 300 researchers in 20 countries publish hundreds of reports, articles and points of view every year. Our thought-provoking research developed with world leading organizations helps our clients embrace change, create value, and deliver on the power of technology and human ingenuity.

Disclaimer