Deloitte. Insights

Cloud sovereignty: Three imperatives for the European public sector

Public sector institutions across Europe must move to the cloud eventually, but can the European Union help them navigate geopolitical tensions, security risks and stakeholders' needs while also fostering EU-driven cloud initiatives?

ARTICLE • 15-MIN READ

Introduction

Concerns around sovereignty usually arise when it is threatened. The recent global geopolitical situation, with conflicts occurring in Europe and the Middle East, intensifies the relevance of sovereignty as a discussion topic among policymakers. While in the past, sovereignty referred solely to the physical borders of a country or its assets, these days, it has gained a digital dimension and includes issues such as cloud and digital sovereignty.

For Europe, concerns surrounding digital sovereignty have a dual imperative. The first strand is ensuring that the local cloud market continues to develop as a catalyst for economic prosperity and technological innovation. The second involves navigating the

corridors of global tech diplomacy, particularly when forming partnerships with hyperscalers – most of whom call the United States home. Here, the challenge is to foster a partnership that respects Europe's security prerogatives.

The European cloud computing market is big and will keep growing. According to one benchmark, the European public cloud services will spend about $150 billion on cloud computing by the end of 2023, significantly more than the $110 billion spent in 2022.[1]

Furthermore, the European Commission has adopted the Digital Europe Programme and will invest more than €900 million between 2023 and 2024 on projects that utilise digital technologies like advanced digital skills, AI, cloud computing and data. This suggests that the European Union and, increasingly, more governments are recognising the benefits of cloud adoption and are investing in cloud technology to improve their operations and service delivery. This is bringing tangible advantages to innovation ecosystems, open standards, small and medium-sized enterprises (SMEs), cities, public services and the environment.[2]

The broader digital transformation of Europe is driven by cost-effective IT solutions, hybrid work and innovative services. This and the explosion of data consumption is spurring many European businesses to invest in the cloud to improve governance and security. It is also in response to privacy regulations, digital legislation and regulatory compliance needs as using data at scale raises data compliance, protection and security issues.

These themes also confront the public sector. Accordingly, public institutions' critical requirements and expectations from the cloud environment are changing to meet the needs of citizens and stakeholders.

Figure 1

Needs and expectations of public sector stakeholders

Area of concern	Needs of public institutions	Offerings of cloud computing
Security, data privacy and resilience	• Need robust security measures to protect sensitive information.	• Provides robust security and data protection features that comply with domestic and international laws and regulations.
Cost efficiency	• Are looking for ways to manage their budget allocations and maximise their impact efficiently.	• Offers cost-effective solutions for storing, managing, and processing data. • Prevents public institutions from high capital costs of purchasing and maintaining IT infrastructure.
Scalability, flexibility and interoperability	• Require the ability to quickly and easily scale up or down their IT resources and call for seamless integration of systems.	• Provides the ability to add or remove resources effortlessly as needed. • Enables interoperable systems and reduces the need for manual processes.
Data analytics and decision-making	• Rely on data analytics to make informed decisions and enable data-driven decision-making.	• Offers powerful tools that help institutions analyse large amounts of data in real time.
Collaboration and remote work	• Need to provide access to applications and data to their employees anywhere, anytime.	• Enables remote working and collaboration by providing secure access to firm resources.

Source: Deloitte analysis, 2023.

Setting the scene: The geopolitical landscape for the cloud environment in the EU

Walking the fine line of digital sovereignty: ensuring data security while promoting economic growth

As cloud adoption accelerates across Europe, so do the concerns regarding sensitive information. The volume and importance of data processed by public sector institutions are increasing, so the measures to protect and control this information need to be robust.[3] This was addressed by the European Commission President, Ursula von der Leyen, in her agenda for Europe: "It may be too late to replicate hyperscalers, but it is not too late to achieve technological sovereignty in some critical technology areas."[4]

The hyperscaler landscape of appealing innovative solutions is dominated by US cloud service providers (AWS, Microsoft Azure, Google Cloud and Oracle). Recently, some

Asian companies (Alibaba Cloud) have joined their ranks. However, this does not mean European countries need to sacrifice security and sovereignty, but it does highlight the need for them to bring concerns regarding data access and storage to the table.

Europe has a need to balance data security with economic growth through digitalisation, and to invest in the most advanced technology without compromising security. European Member States and regional governments are imposing regulations and restrictions due to concerns over citizens' data protection and national security.

Although strong data protection regulations are essential to ensure data is secure, it is also vital to promote growth and innovation if Europeans are to match the scale of foreign providers[5] when it comes to the cloud. Recently, Ireland's data regulator issued Meta with a record-breaking fine of €1.2 billion in a significant ruling. The regulator also directed Meta to cease transferring personal data from the European Union to the United States. This landmark decision deemed such data transfers as unlawful.[6]

Europe has signalled that not complying with data protection regulations has implications. However, overprotection can be counterproductive. So, how are European countries walking the fine line between security and overprotection?

Data and digital sovereignty

The global race to develop innovative technologies and fears of losing strategic technological assets has fuelled sovereignty discussions in several economies. In the European Union there is a clear push for digital sovereignty, with pronounced support for policies that boost Europe's leadership and strategic autonomy in the digital space.

The current dominance of non-European tech companies, which often do not offer enough visibility into their compliance with EU values and principles, threatens EU citizens' control over their personal data. This may also affect the growth of EU tech players and diminish the EU's ability to enforce its laws and regulations.[7] To avoid lagging, digital policy has been a priority for the European Commission, with President Ursula von der Leyen pledging that Europe must achieve "technological sovereignty" in critical areas.[8]

As a result, policymakers have been designing mechanisms and measures to foster innovation in Europe and counteract a potential dominance of non-European tech companies, including financial and legal instruments. As a significant strategic asset for the EU economy, cloud computing is a crucial part of this sovereignty push

The third way: fostering European solutions

Europe has three approaches to the dominance of foreign global cloud providers: one is to work with hyperscalers and emphasise the paramount importance of European

concerns. The second is to turn to local cloud services. The final is to keep data in-house and foster European solutions.

Countries like France and Germany are working with local cloud providers[9] to ensure compliance with local regulations. Other countries have started investing in their own cloud infrastructure to safeguard control over their data and citizens' privacy by addressing the needs of the public sector, as well as essential infrastructure operators and companies of all sizes operating in strategic or sensitive areas of public interest.[10]

To ensure regulatory compliance, some organisations are also looking into creating regional sovereign clouds, i.e., a sovereign data space. Germany and Spain will house the first two sovereign regional clouds, launched by Oracle Cloud Infrastructure (OCI), for the European Union. They will serve only EU residents and legal entities and operate separately from OCI's existing public regions in the EU, located in Amsterdam, Frankfurt, Marseille, Milan, Paris and Stockholm. The policies will dictate how data is accessed, handled and stored in the event of government requests.[11]

Political tensions and conflicts

Continued political instability adds significant complexity to the choice of cloud service providers, with organisations having to consider the diplomatic risk of the different offerings.

Recent years have been marked by events that heavily disrupted global supply chains and drew attention to their lack of resilience. As Europe was still reeling from a pandemic crisis, Russia's invasion of Ukraine and a dramatic rise in inflation that quickly spread across economies further strained the international order.

Power dynamics between global regions have been shaping technological spheres of influence and fragmenting the ICT industry through tariffs, taxes and restrictions on digital technology-related services.[12] The accelerating competition is witnessed in the cloud computing market as different regions implement policies to maintain control over their data and critical cloud infrastructure, ensure autonomy and strong

innovation capacity, and prioritise its companies' economic prosperity over foreign industry giants.

The conflict in Ukraine also demonstrates how technology can be weaponised, with cyberattacks on critical infrastructure and cloud computing services being heavily impacted by security breaches. Russia also claims to be the victim of similar attacks. Some cloud providers, including Azure, AWS and Google Cloud, have supported Ukraine by ensuring the continuity of critical government services while withdrawing from Russia. This highlights the vulnerability of government workloads and service continuity to political changes and why relying and depending too much on foreign cloud providers can worry public institutions.[13]

Regulatory landscape

The current regulatory landscape in the EU and the US is complex and constantly evolving – data privacy laws and regulations are challenging organisations looking to implement cloud solutions. Digital sovereignty, in particular data sovereignty, has been a response to the privacy and cybersecurity concerns of European countries.

In 2018, the Clarifying Lawful Overseas Use of Data (CLOUD) Act established that US authorities and federal agencies could access data stored by US Cloud service providers in other countries for national security reasons. The US CLOUD Act conflicts with the EU's General Data Protection Regulation (GDPR), which applies to all companies, regardless of their location, that collect or process EU's citizens' personal information and compromises the digital sovereignty Europeans are trying to achieve.

To an extent, some major cloud service providers have adopted the EU rules. However, Europeans have a dilemma: the need for the cloud to remain competitive internationally versus the loss of dynamics and simplicity with huge workloads.[14] Aiming to solve this dilemma, the Gaia-X initiative was developed. It started with the French and German Ministers of Economic Affairs, who prioritised boosting the cloud sector in their countries. They agreed on a common approach to develop the European cloud infrastructure and data ecosystems.[15]

Gaia-X is not a regulatory framework but a set of guidelines and technical specifications to create a common data-sharing and management framework across different cloud providers and services. It is designed to promote interoperability, open standards and transparency, and to ensure that data is kept secure and compliant with relevant regulations, such as the GDPR.

It consists of a network and secure data infrastructure compliant with European standards in terms of digital sovereignty and innovation. Its aim is not to build European hyperscalers or a sovereign cloud but to "connect different elements via open interfaces and standards to aggregate data and create a platform for innovation"[16] promoting the use of cloud services without compromising privacy and security.

Moreover, it brings together various stakeholders from different sectors to collaboratively develop and promote the Gaia-X ecosystem. Its collaborative nature allows a diverse range of participants to contribute to its development and ensure the success of the European data infrastructure. OpenNebula, an open-source cloud computing platform, is an example. It provides Edge computing open-source platforms to the European Union[17] and joined Gaia-X to contribute its expertise.

Cloud sovereignty: what does it entail?

Cloud sovereignty can be described as the sum of the business-related, political and technological dimensions of data protection and security, as well as the control of and independence from communications, data, infrastructure, operations and software providers. A sovereign cloud must combine governance, strategy and technical controls to ensure autonomy, flexibility, reliance and compliance with regulatory requirements.[18]

It enables organisations to **control, manage and own their computing resources, data and workloads in the cloud** within a specific jurisdiction, ensuring regulatory compliance and without being dependent on service providers. However, there is not a single, widely accepted definition of cloud sovereignty, and it can be differently perceived by different countries and even organisations within the countries.

The cloud sovereignty framework

To evaluate technical cloud sovereignty in organisations, we developed a comprehensive framework covering the entire cloud stack that includes four domains. This framework applies to organisations across all industries, including the private and public sectors. It can be used to assess an organisation's level of maturity in cloud sovereignty, which is imperative before starting on this journey.

Figure 2

The cloud sovereignty framework – four distinct dimensions to map your journey

Source: Deloitte analysis, 2023.

Deloitte. Insights | deloitte.com/insights.com

The framework further includes subdomains that detail the requirements of the main domains. By doing this, organisations can better understand the challenges of adopting sovereignty in the cloud and focus investments on the organisations' unique sovereignty needs and objectives.

As you embark on your sovereignty journey, you will inevitably face challenges across the framework. The following figure shows where these could lie and what strategies and considerations will help you overcome the hurdles and stepping stones.

Figure 3

Navigating the framework: Challenges, strategies and considerations

	Challenges to master	Strategies to leverage	Considerations to observe
Operational sovereignty	• Keeping up **operational efficiency** while still complying with **sovereignty principles**. • Ensuring **operational sustainability** by leveraging **hybrid and multi-cloud capabilities**. • Increasing **resilience** by adopting remote locations and distributed systems to **avoid disruptions**. • Maintaining **operational consistency** by avoiding a **sprawl** of cloud management tools.	• **Leverage alliances** with service **providers** (sovereign public clouds). • Implement **sovereign landing zones** to enforce regulatory compliance. • Leverage **cloud management tools** agnostic to providers to simplify the operating model for metacloud **abstraction**. • Implement sovereignty-focused governance to evolve the **operating model**.	• The **positive impact** of implementing sovereignty strategies **must justify** increased expenses. • Using **less innovative capabilities** (serverless, managed services) in favour of **higher control** can be a legitimate approach. • You may face **complexity growth** in multi-cloud environments due to system integrations. • Your **resilience strategy** needs to **consider political upheaval**, **compliance** and **foreign** vendor contractual **relations**.
Data sovereignty	• **Enforcing data privacy** regulations can be difficult. • Ensuring **data integrity** so that data has not been tampered with or compromised. • Maintaining active authorisation of **data access** to users based on data sensitivity and confidentiality levels. • **Data residence** - being aware of where the data is stored, how it is protected and who is accessing it.	• Control of data can be achieved through several measures, such as **data access control, classification** and **encryption**. • Traceability can be achieved through **access control policies** and **immutable audit logs**. • **Geofencing** can ensure the data is stored and accessed only in a specific geographic region. • Using **open standards** to store data can guarantee portability.	• Staying on top of **data privacy** and **security regulations** can require high effort. • **Data classification** and labelling require capabilities of data governance. • **Data anonymisation**, **encryption** and **masking** are fundamental to ensure data security and integrity controls that protect data from being tampered with. • **Latency** and **resilience** must be considered when using **external critical management systems** and hardware security modules.
Software sovereignty	• **Changes in software licensing** can lead to significant legal liabilities. • Long chains of dependencies and backwards-compatibility issues **contribute to reduced portability**. • Proprietary software minimises the capacity to control **maintenance** and **versioning capabilities**. • Difficulties in **repatriating** software-as-a-service/platform-as-a-service products.	• Develop **containerised applications** to foster portability between environments and to avoid vendor lock-ins. • To avoid relying on third-party proprietary IP, build your software stack on **open-source or in-house technologies**. • Formulate clear **exit strategies** for software assets and plan redeployment of software assets. • Conduct **software classification** to determine where the software can be deployed.	• Assess the **pros and cons of having 'off-the-shelf' software** with industry standards, clear liabilities vs. open source. • Get an overview of different **service offerings** by providers and the compatibility with open-source alternatives. • Manage internal software **intellectual property** in sovereign **data stores**. • Focus governance on the **classification of software** by criticality and **compliance evaluation** to regulations.
Infrastructure and communications	• Align infra/comms provider with sovereignty goals to help enable **operational compliance**. • Manage technological **complexity** of the multiprovider, **edge-cloud continuum**. • Ensure infra/comms can fulfill technological **requirements** of **specific industries** (e.g., confidential computing for critical national infrastructure).	• Use **open standards** of infrastructure and communications to enforce **data integration** and **enable interoperability**. • Leverage existing **hardware and hypervisor hardening solutions** from cloud CSPs. • Reduce compliance complexity by **outsourcing to local** infra/comms **providers** to fulfill local jurisdiction laws. • Develop a **catalogue of infrastructure** in case of specific industry requirements.	• Deployment must be based on the organisation's requirements of **data confidentiality** and **sensitivity**, and **regulation, decentralisation**. • **Maturity** assessment of the **infra/comms ecosystem** enables dependencies with other sovereignty layers to be identified. • **Open-source** infrastructure might **require** more **security capabilities** for **critical workloads**.

Source: Deloitte analysis, 2023.

Deloitte. Insights | deloitte.com/insights.com

Three imperatives of cloud sovereignty

Setting public institutions on the path to cloud sovereignty by understanding how it can impact cloud adoption

To address geopolitical and regulatory constraints and keep their European market share, US hyperscalers have announced sovereign cloud offerings that ensure compliance with European laws and regulations. Microsoft Cloud is set to announce their 'boundaries' for sovereignty "providing an additional layer of policy and auditing capabilities that will address individual public sector and government customer needs."[19]

AWS is committed to offering its customers the most advanced set of sovereignty controls and features available in the cloud having made the AWS Digital Sovereignty Pledge. Google "unveiled *Cloud on Europe's Terms*, an ambitious commitment to delivering a cloud stack that provides the highest levels of digital sovereignty while enabling the next wave of growth and transformation for European organisations."[20] Oracle is also working on a 'Sovereign Region' and 'Gov Region' concept to comply with EU regulations and domestic government requirements fully.

Organisations' growing interest in ensuring sovereignty and adopting successful cloud strategies to face the changing needs and expectations of the cloud environment has led us to define three imperatives as critical factors. These factors set public sector institutions on the path to cloud sovereignty by understanding how it can impact cloud adoption.

Imperative 1 – Embrace the cloud sovereignty journey

Cloud sovereignty is a journey rather than a destination and is embraced differently by each organisation to address unique constraints, priorities and requirements. All of these shape the approach to cloud sovereignty. It is essential to recognise that cloud sovereignty is not a one-size-fits-all concept, and different organisations require different levels of control and reliance on cloud services.

While achieving complete sovereignty from external cloud providers may seem desirable, it is often not practical or cost-effective for organisations. Being 100% independent would require significant investments in building and maintaining an extensive on-premises infrastructure and communications, which can be prohibitively expensive. Therefore, balancing control with leveraging the benefits of cloud services

provided by trusted partners is fundamental. This is crucial since building these relationships enables public sector organisations to maintain control over their cloud assets and data while leveraging innovation and the specialised expertise and resources these providers offer.

Another factor to consider is operational autonomy. While public institutions may rely on external providers for certain cloud services, maintaining operational autonomy ensures that critical decision-making and control remain in the hands of the organisation itself. This autonomy allows them to shape their cloud strategy, choose appropriate service models, determine data storage locations, and set access controls according to their needs and compliance obligations. By retaining operational autonomy, organisations maintain more control over their digital infrastructure, mitigate vendor lock-in risks and can adapt their cloud strategy as their needs evolve.

Finally, cloud sovereignty alone does not guarantee increased resilience and is not solely about its technical aspects. Still, it is deeply connected to the concept of digital trust – it encompasses the ability to ensure that data and applications are handled and protected in a manner that aligns with the organisation's requirements. Organisations can establish a robust cloud sovereignty ecosystem that fosters data security, regulatory compliance, and long-term resilience by prioritising digital trust, working with trusted partners, and maintaining operational autonomy.

Imperative 2 – Address the regulation gaps and uncertainty

It is crucial to note that compliance with regulations doesn't automatically equate to achieving "optimal sovereignty." While adhering to regulatory requirements is crucial for organisations, it is important to recognise that compliance alone does not guarantee full cloud sovereignty. Regulators often lag the dynamic cloud market, and their regulations may not encompass all the intricacies and nuances of cloud services. Compliance should be seen as a baseline, while sovereignty requires exceeding minimum requirements to address and manage additional factors during the journey.

Sovereignty extends beyond compliance, particularly in the public sector, where multiple factors apart from regulations come into play. Geopolitical considerations, such as data residency and sovereignty requirements and national security concerns, influence decisions regarding where and how data is stored and processed. Achieving cloud sovereignty in the public sector involves balancing compliance obligations with these broader factors and making strategic choices that align with national interests.

The evolution of cloud computing poses new challenges to regulators. As the cloud landscape expands, with the emergence of artificial intelligence, distributed architectures and edge computing, traditional regulations may struggle to keep pace. Although the EU is leading regulations globally, European regulators must adapt and manage the multi-cloud and hybrid edge-continuum, ensuring that compliance frameworks can effectively cover the spectrum of cloud services and deployment models alongside their evolution.

The goal is to establish a seamless and single control plane that streamlines technical compliance across various environments, transcending environment-driven or ad-hoc regulations. Regulators must work collaboratively with industry stakeholders to understand the evolving technological landscape and develop regulatory frameworks that foster innovation while safeguarding data protection, privacy and security.

Summing up, compliance with regulations is a foundational aspect and the starting point of the cloud sovereignty journey, but it does not encompass its fulfilment. Organisations, particularly in the public sector, must consider additional factors such as geopolitics, interoperability and resilience. Regulators face the challenge of adapting regulations to the evolving cloud landscape and managing compliance across diverse environments. By embracing a broader perspective and collaborating to develop actionable regulatory and legal frameworks, stakeholders can navigate the complexities of cloud sovereignty and foster a compliant, resilient and secure cloud ecosystem compatible with digital innovation.

Imperative 3 – Invest strategically to foster control and ownership

This imperative concerns the organisations' ability to ensure control and ownership over their data and applications hosted in the cloud. Both profoundly connect and reinforce each other, encompassing key aspects like control over critical management systems, devices, intellectual property licensing, protocols, etc.

Control of devices, particularly concerning the semiconductor industry, is one of the critical aspects. This industry is vital in providing the underlying hardware components for devices used in cloud computing environments. Organisations need control over the devices they use to ensure the performance, reliability and security of their operations.

Having control over devices is crucial, but having control over the data itself is equally essential. Public institutions must ensure that they have ownership and control over their data stored in the cloud. This includes accessing, deleting, modifying or transferring the data as required. Data sovereignty is of paramount importance as organisations must control where their data is processed, stored and transmitted to ensure jurisdictional control.

Intellectual property (IP) is another crucial consideration. As organisations embrace new advanced telecommunications technologies (such as, for instance, 5G or 6G), IP licensing agreements play a significant role in determining control and ownership over proprietary technologies. It is essential to carefully address IP licensing terms to protect an organisation's intellectual property, maintain control over critical innovations and ensure the sustainability and development of their products or applications for the future.

Public sector organisations can retain control over their technological advancements by securing favourable licensing agreements to establish a competitive advantage and drive further development and innovation in the cloud ecosystem.

The specific measures and best practices in data security should protect the data processed, stored and transmitted to the cloud environments, including proper encryption standards and Key Management Systems (KMS) acting as key drivers for gaining data control up to stringent standards. With the increasing importance of data

security and privacy, KMS enables organisations to control and manage the encryption keys used to protect their sensitive data stored in the cloud.

By maintaining control over encryption keys, organisations can enforce strong encryption practices, ensure the confidentiality and integrity of their data and manage key distributions. Additionally, external KMS are also a stringent mechanism to manage keys out of the hyperscalers' environment and to offload the complexity and responsibility of key management to trusted third-party providers.

Conclusion

Our imperatives for cloud sovereignty emphasise the need for the public sector to prioritise data security, regulatory compliance and maintaining control over their cloud infrastructure. This addresses the second strand of Europe's digital sovereignty concerns – security issues that stem from working with hyperscalers from outside the region.

In terms of the first strand, ensuring that the local cloud market continues to develop European solutions so the region can advance economically and does not lag on key technologies, it is crucial to acknowledge that directly competing with hyperscalers is not a realistic goal for Europe in the short term, given their significant lead in the market. Instead, the focus should shift towards ensuring survivability, revisiting strategies and aligning policy and investment priorities with the sovereign industry while ensuring proper partnerships for cloud sovereignty.

By embracing a forward-thinking approach that highlights adaptability and aligns with Europe's unique strengths and capabilities, European public sector organisations can thrive in the evolving cloud landscape. Collaboration between the public and private sectors is essential to develop sustainable cloud solutions, foster innovation and promote economic growth.

With a concerted effort to prioritise the needs of European businesses and protect cloud sovereignty, Europe can establish a strong position that balances competitiveness, compliance and resilience in the global cloud ecosystem. By doing so,

Europe can drive the sustainable growth of its digital economy, promote digital trust and safeguard its citizens' interests.

BY **Jean Gil Barroca**
Portugal

Bruno Silva Batista
Portugal

Alfons Buxo Ferrer
Spain

Endnotes

1. IDC, European cloud spending will reach $148 billion this year, despite tug of war effect caused by economic pressures, 9 February 2023.

   View in Article

2. European Commission, €1.3 billion from the Digital Europe Programme for Europe's digital transition and cybersecurity, 24 March 2023.

   View in Article

3. European Parliament, *Digital sovereignty for Europe*, accessed 11 October 2023; Bitkom, *Key points - A sovereign cloud and data infrastructure for Germany and Europe*, 15 November 2019.

   View in Article

4. Ursula von der Leyen, *A Union that strives for more - My agenda for Europe*, European Union, 11 October 2023.

   View in Article

5. Kenneth Propp, Waving the flag of digital sovereignty, Atlantic Council, 11 December 2019.

   View in Article

6. Molly Killeen, Meta hit with €1.2billion fine, ordered to halt EU-US data transfers, Euractiv, 22 May 2023.

   View in Article

7. European Parliament, *Digital sovereignty for Europe*.

   View in Article

8. European Parliament, *The von der Leyen Commission's priorities for 2019-2024*, accessed 11 October 2023.

View in Article

9. Mathieu Rosemain, Deutsche Telekom joins France's OVHcloud to take on U.S. cloud computing giants, Reuters, 14 September 2020.

View in Article

10. OVHcloud, T-Systems and OVHcloud cooperate for Gaia-X, 14 September 2020.

View in Article

11. Scott Twaddle, Introducing Oracle's sovereign cloud regions for the European Union, Oracle, 11 July 2022.

View in Article

12. Gartner, Top 4 trends are shaping the future of public cloud, 11 August 2022.

View in Article

13. Cliff Stanton, Russia and Ukraine are weaponizing cloud technology amid conflict, *Security Magazine*, 13 April 2022.

View in Article

14. Bundesministerium fur Wirtschaft und Klimaschutz, The Gaia-X Ecosystem - Sovereign data infrastructure for Europe, accessed 11 October 2023.

View in Article

15. Janosch Delcker and Melissa Heikkila, Germany, France launch Gaia-X platform in bid for 'tech sovereignty,' *Politico*, 4 June 2020.

View in Article

16. Bundesministerium fur Wirtschaft und Klimaschutz, The Gaia-X Ecosystem - Sovereign data infrastructure for Europe.

View in Article

17. Alberto P. Martí, OpenNebula joins GAIA-X as Day-1 Member, Open Nebula, 19 November 2020.

View in Article

18. Deloitte, Cloud sovereignty - Driving resilience and adaptability through cloud sovereignty, accessed 11 October 2023.

View in Article

19. Microsoft, Microsoft Cloud for sovereignty, accessed 11 October 2023.

View in Article

20. Adaire Fox-Martin, Advancing digital sovereignty on Europe's terms, Google Cloud, 12 October 2022.

View in Article

Acknowledgments

The authors would like to thank **John Smith** of Deloitte Consulting LLP for his contributions to this article. They would also like to thank - **Alvaro Martin**, **Andreas Schwall**, **Bram De Schouwer**, **Didier Descombes**, **Inês Fernandes Neto** and **Sébastien Scholaert**.

Cover image by: **Rovinya Sollitt**
