IDC White Paper

Trusted Cloud: Overcoming the Tension Between Data Sovereignty and Accelerated Digital Transformation

March 2022

Authors:
Archana Venkatraman
Carla Arend
Ralf Helkenberg

Sponsored by AWS

IDC #EUR148953922

Introduction

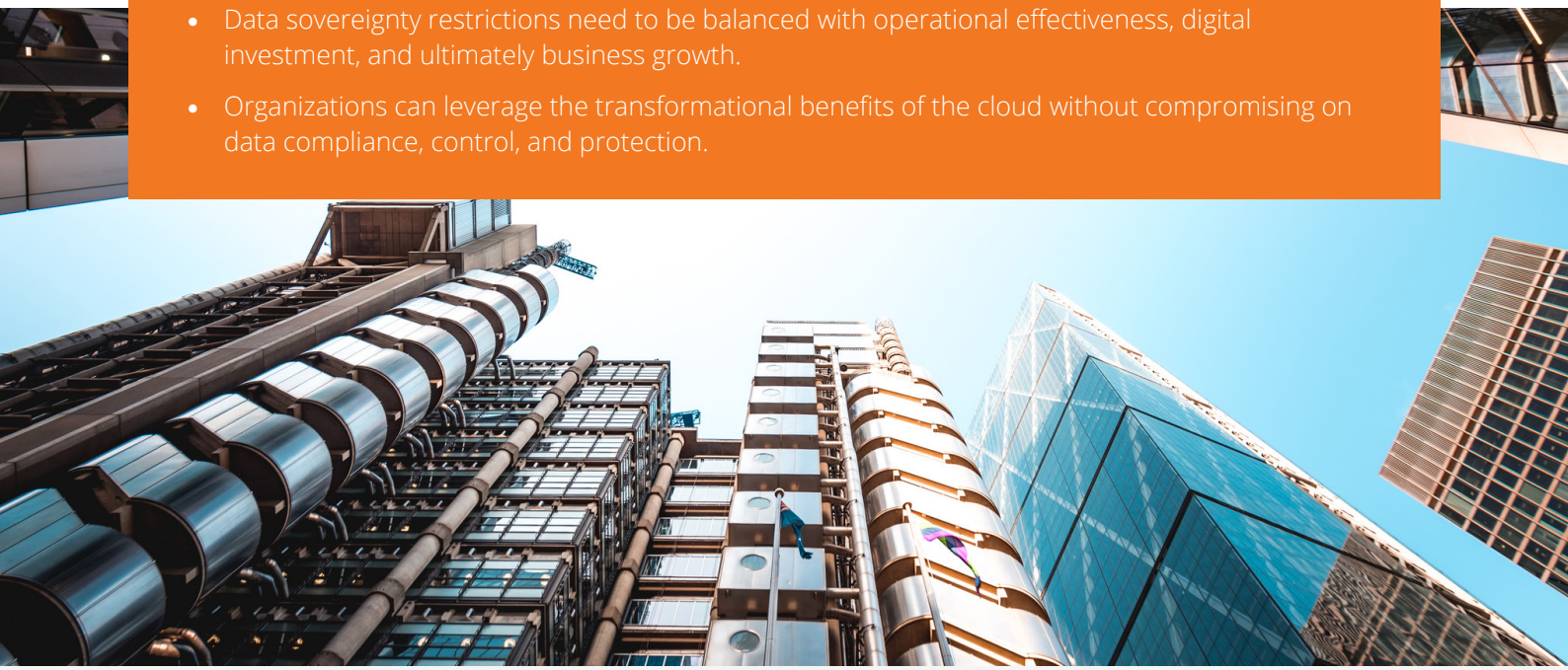
The digital economy is rapidly growing, and IDC predicts that **70% of CEOs of large European organizations will be incentivized to generate at least 40% of their revenues from digital by 2025**. The success of European organizations as participants in the global digital economy depends on their ability to collaborate and share data across borders to drive digital innovation and build new revenue streams from digital products and services. They are turning to cloud platforms to enable digital innovation and data sharing.

However, there are emerging European political concerns about digital and data sovereignty. Data sovereignty is being used by policy makers and regulators to anchor a variety of regulations and governance structures that ensure continued jurisdictional control over data. The growing extraterritorial application of data governance laws is subjecting organizations to increasing tension between enabling digital innovation to accelerate and ensuring data and IT infrastructures are compliant with regulations and guidelines. The data sovereignty implications extend to the European cloud environment given that governments and organizations are increasingly moving their services and data on to platforms managed by international cloud providers.

It is important to distinguish between digital sovereignty and data sovereignty. Digital sovereignty is defined as the capacity for digital self-determination by states, companies, or individuals. It focuses on the control over data, infrastructure, and software that are created and relied on to operate in the digital world.

KEY TAKEAWAYS

- European organizations currently spend more on public cloud than on core datacenter infrastructure.
- Data sovereignty lays out the laws and governance structures within the nation that data is collected in or pertains to.
- Data sovereignty restrictions need to be balanced with operational effectiveness, digital investment, and ultimately business growth.
- Organizations can leverage the transformational benefits of the cloud without compromising on data compliance, control, and protection.



Data sovereignty is a subset of digital sovereignty. It is the concept of data being subject to the laws and governance structures within the country it is collected or pertains to. When dealing with on-premises infrastructure, data sovereignty is clearcut. It is a more complex issue though when it comes to storing and processing data in the cloud.

In this IDC White Paper, IDC discusses the impact of data sovereignty initiatives in the context of digital innovation and cloud adoption in the digital economy. The paper:

- Provides an overview on how cloud adoption in Europe is becoming an enabler of digital transformation, innovation, and business growth.
- Reviews the key data sovereignty concerns and measures, and their impact within the context of the cloud.
- Explores how cloud infrastructure vendors are embedding privacy, security, and compliance into their cloud service to address the concerns raised.

The Role of Cloud in Building the Future Digital Enterprise

Welcome to the digital-first world. IDC predicts that 70% of CEOs of large European organizations will be incentivized to generate at least 40% of their revenues from digital by 2025, which means they need to accelerate their digital transformation and transition faster from physical to digital products and services.

To achieve this goal, CEOs need to ensure that their organizations are building new digital capabilities such as data-driven innovation, embedded intelligence, agile innovation culture, resilience, ecosystem collaboration and data sharing, as well as next-generation security capabilities and digital trust.

Cloud platforms are the de facto engine for the digital future.

46% of European CEOs will accelerate the shift to cloud as their most strategic IT initiative in 2022 and 23% of European CEOs see cloud providers as their number 1 strategic partner for their digital future, according to a 2022 IDC survey of 103 CEOs across Europe.

According to IDC's European Multicloud Survey, 2021, about 46% of European organizations said they "currently use any cloud computing technologies extensively" and more than 36% of their infrastructure spend is dedicated to the public cloud — higher than their core datacenter infrastructure spend. IDC estimates that the full cloud spend will cross $1.3 trillion by 2025, growing at a CAGR of 16.9% to 2025.

With growing maturity in both digital innovation and cloud, European organizations increasingly see cloud as a platform for innovation and as an IT operating model bringing speed, scale, and collaboration to their organization, and enabling the new digital culture they are building.

According to IDC research, organizations cited the following top 6 benefits of migrating to the public cloud:

01. Higher business and IT productivity

02. Faster application and digital services deployment

03. Ability to deliver better customer experience/retain customer loyalty

04. Access to cloud-based ecosystem innovation

05. Faster time to market

06. Increased revenues and profit

These business outcomes highlight the foundational role of public cloud in meeting business growth, adaptability, and innovation objectives. The growing value of cloud in business transformation can be attributed not just to the speed of new features and service innovation but also the capabilities that cloud providers add to help organizations meet evolving legal requirements around security, data protection, and access controls when using cloud services.

Building a Foundation for Successful Cloud Adoption

With cloud becoming a preferred platform for both net-new workloads as well as existing data-intensive and business-critical workloads, the demands from cloud platforms are high. There is no one route to cloud and there is no big bang approach to cloud adoption. Migrating to the cloud can be a multiyear journey and be driven by different business objectives, ranging from datacenter consolidation and adopting opex business models to capitalizing on access to next-gen infrastructure security, economies of scale, sustainable infrastructure, and accelerating digital innovation.

However, using the public cloud is inseparably connected to the level of trust in the cloud service provider. There is no doubt that when taking cloud to scale, one of the fundamental requirements is security and data protection compliance. IDC's ongoing research shows that European organizations are moving from a position where they see security as an inhibitor to that of a key driver for cloud adoption.

In a 2021 IDC cloud survey, European organizations cited "better security" as one of the top benefits that cloud brings to their organization and said an improved security posture is one of the big value gains of moving to the cloud. Security capabilities in the cloud have become the gold standard for security because the cloud brings next-generation infrastructure and logical security, secure network, tiered access and identity controls, and data loss prevention capabilities.

By leveraging the strong next-gen security capabilities around infrastructure security as well as end-to-end encryption and strong access controls, organizations find they can mitigate many security and data protection risks and focus on issues such as business logic and business data management.

Lack of in-house cloud security expertise remains an ongoing challenge. IDC research highlights security as the key area organizations need help with when migrating to the cloud. While cloud providers offer high levels of security and compliance services, the ultimate responsibility is with the end-user organization, which can struggle to understand the overall security, risk, and compliance implications of using cloud as part of its entire IT estate.

The rising debate around digital and data sovereignty in Europe is forcing European organizations to reevaluate their cloud security and compliance posture. Against this backdrop, it is important to understand the issues on data sovereignty and what to consider when planning your cloud security and compliance approach.

Data Sovereignty and the Cloud

Data sovereignty is the concept of data being subject to the laws and governance structures within the country it is collected or pertains to. When dealing with on-premises infrastructure, data sovereignty can be more clearcut — a more complex issue though when it comes to storing and processing data in the cloud.

Much of the cloud data sovereignty discourse centers on:

- The extent to which foreign government and law enforcement can legitimately access and request customer data stored extraterritorially.
- The extraterritorial reach of foreign intelligence and surveillance programs authorized under national security laws and the level of protection afforded to individuals' privacy, either in-country or once their data is transferred to another country. The Schrems II decision and its focus on U.S. government surveillance laws has left many organizations grappling with whether they can legally and safely transfer data outside the EU, in particular to the U.S.

Law Enforcement Reach: Demystifying the CLOUD Act

A common misconception with regards to the Clarifying Lawful Overseas Use of Data (CLOUD) Act is that organizations that store data in cloud resources owned by U.S. providers could see their data accessed by U.S. agencies without their knowledge or consent. The CLOUD Act does not allow law enforcement to extract data directly from systems. Only in limited circumstances and with a judicial mandate can U.S. law enforcement authorities request electronic evidence from service providers, even if it is held outside the United States.

The international dimension of crime is necessitating greater law enforcement cooperation between countries and the structuring of bilateral agreements to facilitate more efficient requests for electronic evidence. Such an agreement already exists between the U.K. and the U.S., with negotiations ongoing on a framework between the EU and the U.S. Where government bodies are involved, it is possible under Foreign Sovereign Immunity law that they are immune to such requests.

To assuage concerns, the leading cloud infrastructure vendors have made strong commitments to protect customer data from inappropriate government and law enforcement requests. These include informing customers of such requests when possible, evaluating the sufficiency and legality of such requests, and challenging them in the courts where they are excessive or in conflict with EU law.

Transparency reporting has emerged as a valuable practice to demonstrate transparency and accountability, with leading providers now publishing regular transparency reports that list the type and number of governmental and law enforcement data requests each company receives. For example, Amazon's Information Request Reports show that in 2021 AWS received worldwide 1,385 law enforcement requests for information (source: latest Amazon Information Request Report, published on January 31, 2022). Only 20 of the total worldwide requests resulted in the disclosure of content information. There were no disclosures to U.S. authorities of enterprise content data located outside the United States. Though a potential risk, enterprises need to balance the possibility of being subject to data access against any cost increase or functionality decrease they may suffer in switching to a local provider.

In the Spotlight: Surveillance Laws and Data Transfers Under the GDPR

Although data sovereignty is not specifically mentioned within the GDPR, its core concepts are specified, in recital 101 and in Chapter V (Articles 44-50). The underlying principle is that "the level of protection of natural persons ensured in the Union by this Regulation (GDPR) should not be undermined." And GDPR's extraterritorial jurisdiction is a key element of data sovereignty enforcement.

There are though no explicit data residency requirements under the GDPR. The regulation only sets conditions for transferring regulated data outside the European Economic Area (EEA). Concerns over the scope of intelligence and surveillance activities allowed under U.S. national security laws (Section 702 of the Foreign Intelligence Surveillance Act and Executive Order 12333) led to the European Court of Justice in 2020 invalidating the EU-U.S. Privacy Shield, a framework facilitating cross-border transfers of personal data for commercial purposes. The court furthermore set out revised conditions for transferring GDPR regulated data outside the EEA when using Standard Contract Clauses (SCCs), EU-approved template contracts that bind the contracting parties to certain data protection standards.

The ruling has significant implications for personal data transfers between the EU and the U.S. in that it considerably narrows the way they may take place. **The subsequent European Data Protection Board (EDPB) guidance in 2021 sets out the steps that organizations should follow when transferring personal data to third countries:**

01.	Identify and map all transfers of personal data to non-EU countries.
02.	Determine the appropriate legal mechanism for the international transfer.
03.	Assess the equivalency of data protection laws and practices in the third country. In practice, the assessment revolves around if there is any law or practices in force that may affect the effectiveness of the legal transfer mechanism the data exporter is relying on. The guidance does provide that even if there is problematic legislation, a consideration of the practices in the third country may determine that inappropriate behaviors do not occur or that problematic legislation is not applied and so a transfer may be undertaken. The assessment may also consider the practical experiences of organizations undertaking data transfers in the same or similar sector.
04.	Where required, adopt additional contractual, organizational, and technical protective measures to safeguard against overreaching government surveillance.
05.	Ensure additional protection measures do not break other formal compliance requirements.
06.	Regularly reevaluate the effectiveness of compliance position.

While the EDPB recommendations provide direction, they do not remove the uncertainty around EU–US data transfers. Meeting the recommendations is a challenge even for the most well-resourced organizations and is typically beyond the means of many small and medium-sized organizations. Understanding and synthesizing the positions of different data protection authorities across the EU is adding further complexity.

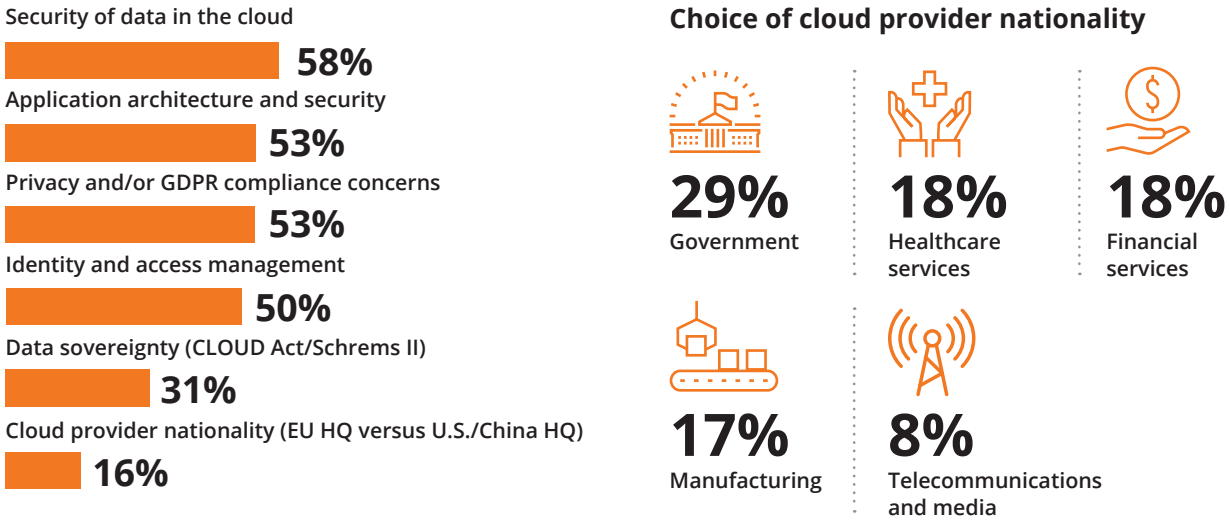
Cloud Data Sovereignty

Cloud data sovereignty is a new and evolving concept and organizations are still at the beginning of understanding its implications on their cloud strategies. **In an IDC survey only 16% of European respondents were concerned about the nationality of their cloud provider, but differences do exist by industry sector** (see Figure 1). Organizations are more concerned about complying with the law than about following not yet very well understood principles of sovereignty.

FIGURE 1

Cloud Computing and Trust

Q. Which aspects of your company's cloud strategy are impacted by concerns over trust?



Source: IDC European Security Survey, 2021

Another reason why fewer respondents are concerned is the costs involved to adhere to the digital and data sovereignty principles.

According to the *IDC Enterprise Resilience Survey* in September 2021, 60% of European organizations agree or strongly agree that digital and data sovereignty increases the cost of doing business internationally.

IDC predicts that over the next four years, 50% of European organizations will spend 10% of their ICT budget to comply with digital sovereignty principles adopted in the EU. The additional spend is expected to cover additional costs and time on infrastructure, data, processes, governance framework, and skills.

At a time when IT budgets are squeezed and organizations want to make IT investments count and deliver business value, they may be tempted to devote resources to more productive outcomes. It is about striking a fine balance between trust and business progress. In IDC's opinion, a key part of the investment should go toward reviewing skills, examining and leveraging existing trusted cloud capabilities, and driving the next phase of workload prioritization for the cloud.

Data Localization as a Risk Mitigation Approach

The Schrems II decision is pushing a Eurocentric approach to data governance. The complexity of making risk assessments on third-country laws and practices, and the need for additional technical safeguards, mean data localization is often the only practical option. In response to the ruling, 64% of respondents in an IDC survey said they were adopting a risk mitigation approach of either holding or being in the process of migrating GDPR regulated data to datacenters located in Europe (see Figure 2).

FIGURE 2

Data Residency in the Cloud

Q. Which one of the following best describes your organization's data residency policy when holding GDPR-regulated data in the public cloud?

35%
Only hold GDPR regulated data in European datacenters

29%
In process of migrating GDPR regulated data to European datacenters

27%
Policy not to hold GDPR regulated data in the cloud

Source: IDC European Security Survey, 2021

A further 42% of European organizations said they were undertaking greater due diligence of their cloud service providers to determine local hosting capabilities and the adequacy of their legal, privacy, and security safeguards.

The leading cloud infrastructure providers are well placed place to support customers' data residency requirements and are continually expanding their European cloud footprints and data residency service features. Because of significant investments in their security capabilities and services, they are also able to provide a level of security that in many cases can't be duplicated onsite.

Security Is Not Increased by Data Localization

The cyberthreat landscape is growing with nation state and cyber criminals increasing the scale, scope, and level of sophistication of their cyberattacks. Security of data in the cloud therefore ranks as organizations' main trust concern when it comes to cloud adoption.

Greater data control and security is often cited as a driver of hosting data in-country. Physical location of the data, however, has no bearing on mitigating data risk to cyberthreats. Any data architecture lacking the appropriate access controls and security protections presents a credible attack opportunity, regardless of location. System misconfigurations from the customer and credential-based attacks are often the source of data breaches. In fact, data residency can run counter to an organization's objectives for security and resilience, for example, for customers who want to use multiple regions for backup and recovery purposes. More and more European organizations are now trusting the cloud for their security needs, as many organizations simply do not have the resources and expertise to provide the same security benefits as large cloud providers.

The Shared Responsibility Model Defines Cloud Security

Organizations don't like the idea of losing control of their data, a concern that extends to multitenant cloud environments. There is the perceived increased security risk of storing data with a third-party provider, the lack of visibility into what data is within cloud applications, and the extent to which they have control over who can access sensitive data.

Cloud data can only be safeguarded if security and compliance features are well understood and properly configured from the outset. The Shared Responsibility Model, by setting out security responsibilities across all types of cloud platforms, provides the starting point and guide to securely leveraging the benefits of the cloud. With the IaaS model, the cloud provider is responsible for securing the infrastructure, including hardware, services, and facilities.

Cloud customers, meanwhile, are responsible for securing the workloads — data, accounts, identities, access, and network configuration — that run on the cloud infrastructure. It's essential that cloud customers fully understand the sliding scale of security responsibilities in the cloud. This also extends to knowing all the security measures delivered by the cloud provider and how to enable them.

Data Access Controls in the Cloud

Cloud providers do not have unrestricted access to customer data in the cloud. Organizations retain all ownership and control of their data. Through credential and permission settings the customer controls who has access to their data. Cloud providers also use a rigorous set of organizational and technical controls based on least privilege to protect data from unauthorized access and inappropriate use. Most cloud service operations, including maintenance and troubleshooting, are now fully automated. Should human access to customer data be required, it is temporary and limited to what is necessary to provide the contracted service to the customer. All access should be strictly logged, monitored, and audited to verify that activity is valid and compliant.

Encryption and Key Management Assumes Greater Importance

Encryption is considered fundamental to data protection best practice and is highly recommended by regulators. Having full control and management over key material is assuming greater importance where organizations are moving sensitive workloads to the cloud. In addressing the Schrems II ruling, the EDPB in its final recommendations on supplementary technical measures for personal data transfers stresses the need for organizations to have full control over their encryption keys.

Cloud service providers offer multiple ways for customers to manage and control encryption, from encrypting data in transit and at rest to customer managed encryption keys, including bring your own key using key management services and FIPS 140-2 or FIPS 140-3 certified hardware security modules. Without exposing encryption keys or sensitive data to the cloud provider, client-side encryption provides the highest level of data control. However, the drawback is severe limitations in cloud service use and functionality. Many cloud applications such as analytical services do not work with this type of encryption because the data content is completely inaccessible and unreadable. Repeated cycles of encryption and decryption of data for use in the cloud may also induce latency issues.

The EDPB recommendations identify certain international data transfer scenarios where no effective technical supplemental measures could be found that would protect data from access by public authorities. This includes where organizations use cloud services situated in third countries without equivalent protections, which require data processing in the clear (unencrypted data). The EDPB does not rule out that further technological development may offer measures that achieve the intended business purposes. Encrypted data processed in memory within hardware-based trusted execution environments (TEEs), also known as enclaves, can alleviate these regulatory concerns by rendering sensitive information invisible to host operating systems and cloud providers. The AWS Nitro System, the underlying platform that runs Amazon EC2 instances, is an industry example that provides such protection capability.

Trusted Cloud Certification Schemes

"Trust but verify" is a good practice when employing a cloud service. Independent accreditations against official standards are a recognized basis for assessing adherence to privacy and security practices. Examples include codes of conduct. Approved by the EDPB, the EU Cloud Code of Conduct and CISPE's Code of Conduct for Cloud Infrastructure Service Providers provide an accountability framework to help cloud service providers demonstrate compliance with their processor obligations under GDPR Article 28. While not required for GDPR compliance, CISPE uniquely requires accredited cloud providers to offer customers the option to retain all personal data in their customer content in the European Economic Area. CISPE Code of Conduct compliance requires a full audit from independent monitoring bodies accredited by the French data protection authority (CNIL).

Privacy and security assurance are also provided through compliance certification to internationally recognized technical and management standards such as ISO 27018, ISO27001, and ISO 27701, independent audit reports (SOC1 and 2), and attestation schemes (C5 Cloud Computing Compliance Controls Catalogue). Independent certifications, attestations, and codes of conduct are helpful to building an environment of trust and transparency in the European cloud computing market and to simplifying the risk assessment process of cloud service providers for customers.

Gaia-X: An Example of an Emerging Data Sovereignty Framework

One emerging example of strengthening data sovereignty and GDPR compliance is the European initiative Gaia-X, which has more than 350 institutions participating in it.

Gaia-X is an initiative to establish a federated and secure data infrastructure. Its goal is to drive innovation through the lens of digital sovereignty by establishing an ecosystem in which data is made available, collated, and shared in a trustworthy environment. Gaia-X is still in the early stages of determining the use cases and it has several public cloud vendors actively participating in the working groups to better serve the privacy and control needs of global companies in a consistent and standardized manner. The data sovereignty principles and safeguards developed under the Gaia-X initiative might find their way into new regulations in the coming years.

Translating Data Sovereignty Requirements Into Actionable Business and IT Strategy

Digital and data sovereignty initiatives have mainly been driven by political leaders and regulators and are expected to evolve over the coming years. For business leaders it is important to understand how they can translate the data sovereignty debate and initiatives into actionable business and IT strategy.

The first step is to understand how data sovereignty relates to the organization's data strategy and its security, risk, and compliance strategy. While the regulatory landscape is constantly evolving, the only tangible points that organizations can take into account right now are the regulations and regulatory guidance outlined above, which they need to adhere to. As a starting point, it is important to perform overall risk assessments of the public cloud versus on-premises infrastructure, and to compare these risk assessments. You need to use your risk profile to determine which risk levels you want to accept. It is impossible to bring all risks to zero, and cloud/outsourcing by design has some different risks than on-premises infrastructure. In the end the net total of the different risk assessments is what matters, and not an isolated assessment of a specific risk out of context.

The second step is to decide how to balance the need for digital innovation with the need for data sovereignty. For public sector organizations, data sovereignty is a key value that they value highly, whereas manufacturing or retail organizations will have a different balance that works for their business objectives and competitiveness. They need to compete in the global digital economy and want to use a global platform that enables digital innovation at speed, while adhering to local regulations as they emerge.

Ultimately, data sovereignty considerations should inform the data strategy of an organization, which starts with data discovery, to understand what data the organization has, where it resides, who owns it, who has access to it, and which regulations govern the use of it.

Organizations also need to attach a value to their data, to see if it is of critical importance for company survival or critical to controlling the company's digital destiny — in which case, the data sovereignty debate and the emerging principles will be important to follow and implement for these specific data sets; different and more relaxed governance policies will suffice for less important data sets.

Action Plan: How to Implement Data Sovereignty Principles

For individual organizations already on a hybrid cloud journey, there are several steps and strategies they can take or capitalize on to strengthen their control over operations, infrastructure, data, and software.

Understand the shared responsibility model to determine which security and compliance measures your cloud provider takes care of and what you need to do to implement your data sovereignty measures. Implementing data sovereignty principles is your responsibility, but your cloud provider supports you with multiple security and compliance services.

Avoid the temptation of sovereignty for sovereignty's sake and determine the value. For most organizations, the outcomes they are trying to gain through such initiatives are strengthening transparency, choice, and control, and to better meet data privacy, compliance, and trust requirements. For most needs, adopting cloud services that deliver next-gen security, hybrid cloud capability, encryption, cleared shared responsibility contract, and data residency options can be a strong start.

Focus on building cloud skills through training. Organizations should prioritize investing in delivering cloud-focused awareness, training, certification, and skills building to use cloud responsibly and efficiently.

Prioritize delivering business outcomes. Data sovereignty principles need to be balanced with business strategy and the need to drive digital innovation. Multiple stakeholders need to be involved to evaluate all aspects of required business outcomes, and the associated cost, governance, and risk tolerance, early on.

Establish continuous checks and controls for compliance and adhere to data sovereignty principles in a way that works for your organization's needs. Cloud is a dynamic environment. Establishing continuous checks and controls helps keep track of how usage and data footprint in the cloud environment is evolving and to keep up with the innovation in cloud platforms that you can leverage to bolster the security and resilience of your IT.

Workload-focused approach to data sovereignty. Organizations should start with their compliance foundation to assess their workloads and understand which data is sensitive (such as personal data, company IP, patents, strategy, confidential, official, or secrets data) and requires a higher degree of management and control. This can be a starting point to establish the risk tolerance and classify workloads as low, medium, and high risk workloads. This means organizations don't have to think of digital sovereignty as a blanket strategy and facilitate an accelerated move to the cloud for low-risk workloads such as IoT workloads, edge workloads, or some speed-sensitive workloads to accelerate innovation. Another advantage of this strategy is that they can concentrate on a portion of workloads to make digital sovereignty initiatives manageable and mitigate their risks.

Consider a hybrid cloud approach. If you are not yet comfortable putting all your data into the cloud, you can always implement a hybrid cloud approach, where some datasets can move to the cloud while others remain in your own datacenter, until the right security and compliance measures have been determined.

Conclusion

A rapidly growing digital economy and the cloud infrastructure that underpins it operate smoothly when they do not have to consider physical borders, data protection regulations, or government interference. However, there are emerging concerns about digital and data sovereignty, and growing tension between allowing digital innovation to accelerate within the cloud, while also ensuring that data, software, and IT infrastructure is governed in a way that ensures organizations comply with national regulations and guidelines. Organizations need to strike a balance between their need to accelerate digital innovation and the requirement to comply with national regulations around the globe.

Cloud infrastructure providers such as AWS understand that customer trust in cloud services is critical. Their platforms are built with security, data protection, and privacy in mind. They continually invest large amounts into core infrastructure protection and the deployment of state-of-the-art security services, including encryption, identity and access management, intrusion detection, network security, and compliance management. Infrastructure and services are constantly subjected to technical security testing by independent experts, as evidenced by the broad set of compliance and standards certifications. The scale of their security capabilities and constant innovation means organizations increasingly view cloud infrastructure environments as more secure than what they can deliver in their on-premises environments.

The cloud security shared responsibility model, however, is inherent to the use of cloud services, and it is essential that organizations fully understand their data protection responsibilities within this. In partnering with a trusted cloud provider such as AWS, organizations can architect and deploy sensitive workloads on their compliance terms and meet their requirements for security, privacy, and data sovereignty — all without losing the transformational benefits of its cloud services.

About the Analysts

Ralf Helkenberg, Research Manager

Ralf Helkenberg leads IDC's European Privacy and Data Security research practice. He covers the evolving regulatory landscape, as well as provides insights into the market dynamics, vendor activities and end-user adoption trends in the privacy management, de-identification and data security markets.

Archana Venkatraman, Associate Research Director

Archana's primary research coverage is cloud data management. She covers multiple topics including data protection, edge to cloud data trends, application and data availability, compliance, data integration, intelligent data management, DataOps, data quality, and multicloud priorities and trends.

Carla Arend, Senior Research Director

Carla Arend is a senior program director with the European software and infrastructure research team, and heads up IDC's European cloud research. Arend provides industry clients with key insight into market dynamics, vendor activities, and end-user adoption trends in the European cloud market. As part of her research, she covers topics such as how European organizations are adopting cloud, cloud security, data management in the cloud, as well as GDPR impact on cloud.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com

Corporate HQ

140 Kendrick Street,
Building B, Needham
MA 02494 USA
508.872.8200
www.idc.com

Copyright and Restrictions:

IDC #EUR148953922