

2024 Data Security
Directions Council

Data Sovereignty: Who Owns Your Data and Can You Control It?





Data Sovereignty in a Connected World: A Balancing Act

Sébastien Cano, Senior Vice President, Cloud Protection & Licensing at Thales, and Moderator, Data Security Directions Council.

The digital age has ushered in a new era of interconnectedness, but with it comes a growing concern: data sovereignty. Businesses across the globe are grappling with the need to harness the power of data analytics while ensuring compliance with increasingly stringent regulations and protecting the privacy of their customers.

The 2024 Thales Data Security Directions Council report, featuring insights from leading global security experts, highlights the complex landscape of data sovereignty. It underlines the importance of striking a balance between leveraging the benefits of cutting-edge technologies, including Artificial Intelligence (AI) and 5G, and maintaining control over sensitive data.

At Thales, we believe data sovereignty is not a barrier to innovation; it's an enabler. We provide businesses with the tools and expertise to navigate this evolving environment. Our cloud-based data protection and key management solutions empower organizations to securely store and process data within their desired geographic boundaries while still reaping the benefits of performance, scalability, and agility offered by cloud technologies.

The security leaders featured in this report offer invaluable perspectives on the challenges and opportunities presented by data sovereignty. Their insights showcase a range of approaches, from utilizing advanced encryption and key management techniques to fostering international collaboration on data residency regulations.

Thales, recognized as a European leader in cloud security and data protection, is committed to being your trusted partner in this critical journey. Our comprehensive portfolio of solutions, combined with our deep understanding of regulatory nuances, ensures your data remains secure and compliant wherever it resides.

By fostering an open dialogue on data sovereignty, we can collectively build a future where businesses can thrive in the digital economy while upholding the highest standards of data security and privacy.



Sébastien Cano

Senior Vice President, Cloud Protection & Licensing at Thales, and Moderator, Data Security Directions Council

As the Senior Vice President of Thales Cloud Protection & Licensing, Sébastien Cano leads a global business focused on helping organizations and the most respected brands in the world protect their most sensitive data, secure the cloud, and create more value for their software in the devices and services used by billions of consumers every day. He is responsible for the business and strategy for the company's industry-leading data encryption, identity and access management, application security and software monetization solutions.

Contents

Council Members	4
Sovereignty in a Globalized, Interconnected Data Environment	7
Beyond Definitions: The What and Why of Data Sovereignty	8
What is Data Sovereignty?	8
The Driving Concerns Behind Data Sovereignty	9
Operationalizing Data Sovereignty: Business Challenges and Legal Complexities	11
What are the biggest challenges businesses face?	11
Data Sovereignty Challenges: The Cloud Providers' Perspectives	15
How do privacy regulations and data sovereignty requirements affect businesses' cloud strategies?	18
The Foundations of Data Sovereignty: Strong Encryption and Effective Key Management	20
Importance of Encryption to Data Sovereignty	20
The Importance of Key Management to Controlling Your Data	23
Selecting the Appropriate Key Management Approach	24
The Impact of Emerging Technologies on Data Sovereignty: Quantum Computing, 5G, and AI	28
The Impact of Quantum Computing	28
The Impact of 5G Technology	30
The Impact of Generative AI	32
Regulate and Innovate: How Legislation Drives Technology Innovation	34
Regulatory Challenges as an Opportunity for Innovation	34
The Rise of Privacy-Enhancing Technologies (PETs)	36
Strategic Insights: Internet Balkanization, Cyber Warfare, and The Future of Data Transfers	37
Internet Balkanization: A Credible Risk?	37
Cyber Warfare and Localized Data Centers	38
What is the Future of Data Transfers?	40
How Thales Enables Data Sovereignty	42
Best Practices for Data Sovereignty Compliance	43
Key Takeaways	44
Data Sovereignty Compliance Checklist	46

Council Members



Agnieszka Bruyère, Vice President of Cloud Growth and Public Sector, Oracle EMEA

Agnieszka oversees both Oracle's Cloud Expansion strategy and Cloud adoption in the Public Sector across the EMEA theatre, with a particular focus on security and compliance to achieve an optimum level of cyber-resiliency and sovereignty. With 23 years of experience in the field of information technology, Agnieszka has built a deep knowledge and has become a recognized expert in the field of cloud & compliance, sharing her experiences and insights through several published articles and interviews.



Alex Meek-Holmes, Senior Manager of Sovereignty and Strategic Infrastructure, AWS

Prior to working in AWS Alex worked in the UK Civil Service. He was most recently responsible for cyber security across UK industry. As Chief Operating Officer of the Government Digital Service he played a key role in the digital transformation of UK government, improving services for citizens and saving billions of pounds. Previously he worked in HM Treasury, where he devised and implemented spend controls, which helped the UK Government move to cloud computing. Alex is also a Policy Fellow at the Royal Academy of Engineering.



Dr. Avesta Hojjati, Head of R&D, DigiCert

Prior to joining DigiCert, Dr. Hojjati held a variety of roles at large enterprises such as Symantec and Yahoo, as well as being a founder and CEO at Security7 Inc., a penetration testing company. At DigiCert, Dr. Hojjati leads the advanced development of a suite of cybersecurity products, including embedded/IoT device security and post-quantum cryptography (PQC) solutions, in addition to influencing the broader product roadmap in conjunction with the M&A strategy. He has authored over 20 journal/conference papers and is the inventor of 30 U.S. patents, both granted and pending.



Ganesh Subramanya, Global Head – Data Security Practice, Cyber Security, Tata Consultancy Services

Ganesh leads the Data Security Practice within TCS' Cybersecurity Business Group, creating solutions for clients to protect business critical data, and ensure compliance to data privacy requirements. He is responsible for developing solutions, platforms and services in technologies like Data Discovery, Data Security Governance, Certificate Management, Data Encryption and Key Management, in collaboration with global partners like Thales. In addition to Data Security Practice, Ganesh also heads the OT & IoT Security Practice.



Kris Lovejoy, Global Practice Leader, Security & Resiliency, Kyndryl

Kris Lovejoy, an internationally recognized leader in the field of cybersecurity and privacy, is the Kyndryl Global Practice Leader for Security and Resiliency. She also serves as the co-sponsor of Kyndryl's ID&E Committee, the "Women's KIN". Kris holds U.S. and EU patents in areas around Risk Management. She was named Consulting Magazine's "Top Woman Technology Leader" in 2020; The Consulting Report's "Top Cybersecurity Consultant" in 2021. She also received the Change-Maker Award by The Cyber Guild in 2022 and was named one of the on "The Top 10 Guardians of Cyberspace for 2022" by Cyber Express.



Michael Tadault, Chief Technologist for Telco in APAC, Red Hat

Michael helps telco service providers become more agile, innovative and efficient by adopting technologies like cloud native development, containers, virtualization and the open hybrid cloud, as well as changing their processes and culture to make the best use of these technologies. Before joining Red Hat Michael spent more than 20 years in the telco industry holding key positions in project management, product management, system integration, presales, and solution architecture across numerous technical domains like fixed/mobile access, transport, core, and OSS/BSS. Michael holds a Masters Degree in Engineering from École Polytechnique and Télécom Paris.



Tony Baudot, Attorney at law, Deloitte Société d'Avocats

Tony is attorney at law in charge of the Digital & Innovation legal practice within Deloitte Société d'Avocats. He assists clients in the private and public sectors with their digital transformation projects drawing on such technologies as AI, the internet of things, Blockchain, Cloud or RPA. Tony also helps his clients manage regulatory risks relating to digital transformations, data protection, data sovereignty, the implementation of complex IT systems or their operation, in particular in the Cloud via managed services, hosting or third-party maintenance providers, both in Europe and internationally.



Mark Hughes, Global Managing Partner of Cybersecurity Services at IBM Consulting

Mark Hughes is the Global Managing Partner, Cybersecurity Services at IBM Consulting, and leads IBM's team of thousands of experts in helping organizations transform security into a business enabler and establish cyber resiliency. His role spans the sales and services delivery of threat detection and response, data security, cloud security, IAM, infrastructure, risk management, and ecosystem partnerships. Before joining IBM, Mark's cybersecurity career spans over two decades, including recent roles as President of Security at DXC Technology, a fortune 500 global technology services provider, and Chief Executive at BT Security, a leading global telecommunications provider. Mark has served on national boards, including the Cyber Growth Partnership for the United Kingdom, and the World Economic Forum's (WEF) Global Cybersecurity Board.



Brian Roddy, Vice President of Product Management, Google

Brian oversees GCP's SaaS security offerings as well as platform work to ensure GCP is the world's most trusted cloud. Brian has more than 25 years of experience in helping build great product, engineering and operations teams. Previously, Brian was the GM of Cloud Security at Cisco, joining via the OpenDNS acquisition. Before Cisco, Brian led the engineering team at Jive Software and was a founder of Reactivity, a web services security company that was acquired by Cisco in 2007. Brian holds a B.S.E. from the University of Pennsylvania and a M.S. from the University of Wisconsin, Madison.



Chris Hickman, Chief Security Officer, Keyfactor

As a member of the senior management team, Chris is responsible for establishing & maintaining Keyfactor's leadership position as a world-class, technical organization with deep security industry expertise. He leads client success initiatives and helps integrate the voice of the customer directly into Keyfactor's platform and capability set. Chris previously held the position of Director of Technical Services at Alacris, an Ottawa based smartcard and certificate management company, which was sold to Microsoft and is now part of the Microsoft Identity Manager product suite. Chris has worked on PKI projects for organizations and firms including NATO, both the U.S. and Canadian Departments of Defense, Fortune 100 banks and financial institutions, manufacturers, insurance companies, telecommunication providers and retailers.



Duncan Jones, Head of Cybersecurity, Quantinuum

Duncan has over 16 years of experience developing security solutions for global companies, with projects ranging from securing the backbone of the Internet to maintaining national ID systems. In his role at Quantinuum, Duncan oversees cybersecurity activities, including the development and commercialization of the Quantum Origin platform, which generates the strongest cryptographic keys in the world using quantum computers. He is a regular speaker and commentator on cybersecurity topics at events and in the media. Duncan is also a member of the World Economic Forum Quantum Cybersecurity Initiative.



Data Sovereignty in a Globalized, Interconnected Data Environment

Is your data truly yours? In today's hyper-connected world, where information flows like electrons, that seemingly simple question carries weighty implications. The answer, however, is far from binary. Enter the complex and sometimes contentious realm of **data sovereignty**.

In an era where data is seen by many as more valuable than gold or oil reserves and digital innovation drives the wheels of global economies, the concept of **sovereignty** has emerged as a critical fulcrum in the balance of power, control, and ethical governance.

For executives like you, data sovereignty is not just another buzzword. Data sovereignty is the cornerstone of digital autonomy, ensuring who accesses and controls data. It involves enforcing data integrity and confidentiality through robust encryption and stringent access controls.

It's a strategic imperative, a regulatory tightrope walk and a potential competitive edge. It's about ensuring control over your most valuable asset – **information**.

But navigating this landscape can be like traversing an uncharted jungle. Governments clash with corporations, privacy concerns tangle with economic opportunities, and technological advancements rewrite the rules every day.

This report is your compass.

Within these pages, you'll find:

- **Expert insights:** We've interviewed leading executives from cloud providers, consulting firms, and service providers, offering perspectives from across the data sovereignty spectrum.
- **Untangling the jargon:** Clear, concise explanations demystify key concepts like data localization, residency, and ownership, empowering you to make informed decisions.
- **Global landscape analysis:** Understand the evolving regulatory environment, from Europe's GDPR to emerging regional frameworks, and how they impact your business.
- **Practical strategies:** Discover actionable steps to achieve compliance, enhance security, and unlock the value of your data, all while navigating data sovereignty complexities.
- **Future-proof insights:** Explore emerging technologies, their impact, and their potential to redefine data control.

Whether you're a seasoned data veteran or a newcomer grappling with the challenges, this report is your guide. We'll equip you with the knowledge to navigate the intricate world of data sovereignty, transforming it from a risk to an opportunity.

Dive in and unlock the true potential of your data. The journey starts now.

Don't just take our word for it. Hear directly from the experts in the following pages as they share their unique perspectives on this critical issue. Their insights will challenge your assumptions and spark transformative ideas.

Ready to take control of your data destiny? Turn the page.

Look out for our checklist at the end of this report to help you review best practices.

Beyond Definitions: The What and Why of Data Sovereignty

Understanding the concept of data sovereignty is essential for any organization operating in the global digital economy. It's not just a buzzword; it's a critical legal and strategic consideration that shapes how we handle and protect data in an interconnected world.

What is Data Sovereignty?

At its simplest, data sovereignty is the principle that digital information is subject to the laws and governance structures of the country in which it is stored as well as where it originates. Council member Tony Baudot, Attorney at law at Deloitte Société d'Avocats', defines data sovereignty as "a country's or the EU's authority to control data within its borders." He further explains that although "data sovereignty is not a legal term defined in a specific law or regulation in Europe, it is becoming increasingly important as we move into a digitalized world."

Data sovereignty is not a trending buzzword. Instead, it is a longstanding issue, centered around questions on data ownership, protection, storage, and ensuring third-party protection of the data in accordance with the owner's requirements.

For example, a business based in the United States must comply with the EU's General Data Protection Regulation (GDPR) if it collects data from individuals in France. Similarly, if the same company gathers data from a customer in California, it must adhere to the California Consumer Privacy Act (CCPA). This complexity is compounded when you consider that 137 out of 194 countries have put in place legislation to secure the protection of data and privacy.¹

"Data sovereignty is a country's or the EU's authority to control the data within its borders."

Tony Baudot
Attorney at law,
Deloitte Société d'Avocats



Data Sovereignty vs. Data Localization and Data Residency

"Data sovereignty is often confused with data residency, which refers to the geographical location of data."

Mark Hughes
Global Managing Partner
of Cybersecurity Services
at IBM Consulting



Data sovereignty should not be confused with data localization or data residency. Mark Hughes, Global Managing Partner of Cybersecurity Services at IBM, also clarifies that "Data sovereignty refers to the laws and regulations governing and controlling data within a specific jurisdiction. It is often confused with data residency, which refers to the geographical location of data."

Data localization is a governmental mandate restricting data transfer outside a specific location. In contrast, data residency is a strategic decision by organizations to store data in a particular geographical area for various reasons, including legal compliance, tax benefits, or performance optimization. Once a location is chosen for data storage, it becomes subject to the data sovereignty laws of that region.

¹United Nations, "Data Protection and Privacy Legislation Worldwide", <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>

The Three Dimensions of Data Sovereignty

Agnieszka Bruyere, Vice President of Cloud Growth and Public Sector, Oracle EMEA, adds a different perspective on the definition of data sovereignty. According to Bruyere, "Data sovereignty has three dimensions: data residency, access to data, and stewardship of data." Besides deciding where to store data, it is essential to determine who can have access to this data, which "becomes more crucial as we consider all the data required for training purposes of AI models." Bruyere also stresses the importance of full stewardship, especially in the context of AI. The critical question for Bruyere is, "Who can access what data outside of the country or the European Union and through cloud operations." These concerns are also at the core of the EU AI Act, which aligns with GDPR to ensure that AI systems adhere to high standards of data protection and privacy.

"Data sovereignty becomes more crucial as we consider all the data required for training purposes of AI models."

Agnieszka Bruyere
Vice President of Cloud Growth
and Public Sector, Oracle EMEA



The Driving Concerns Behind Data Sovereignty

The dominance of a small number of large technology companies is considered the driving force fuelling the urgency of addressing data sovereignty. These companies control vast quantities of user data, giving them considerable influence over privacy, data protection, and the digital environment. This concentration of power raises concerns, particularly in regions like the EU, about the impact on the data economy, innovation potential, and digital security.

A recent IDC survey revealed that 79% of respondents expressed concern about their critical data being managed by US cloud providers. Concerns stem from legislation like the US CLOUD Act, which allows US law enforcement to access data stored by major cloud providers, even if the data is located outside the US.

GDPR further complicates the landscape. Under its terms, any organization, regardless of location, must comply with data management rules to engage with customers in EU countries. These rules empower individual citizens to exert more control over their personal data.

Navigating the maze of data sovereignty is not just a legal obligation but a strategic necessity for businesses. It's about understanding and respecting the nuances of global data laws, being aware of the geopolitical implications of data storage and transfer, and ensuring compliance across different jurisdictions.

In this evolving digital landscape, companies must stay agile, informed, and proactive in their data management strategies. It's not just about adhering to regulations; it's about building trust with customers and partners, ensuring data security, and safeguarding the fundamental right to privacy in a digital world where data knows no borders.



Operationalizing Data Sovereignty: Business Challenges and Legal Complexities

What are the biggest challenges businesses face?

In today's rapidly evolving digital landscape, business leaders across public and private sectors are grappling with the multifaceted challenges of data sovereignty as they navigate complex regulatory landscapes and manage data across multiple cloud environments.

Extraterritorial Impact Shadows Cyber Resiliency in the Cloud

Agnieszka Bruyere brings our attention to a significant yet often overlooked aspect - the impact of extraterritorial laws on cloud usage. The extraterritorial application of laws, such as the United States' CLOUD Act or the European Union's GDPR, has profound implications for businesses leveraging cloud services. These laws often extend beyond the borders of their originating countries, impacting how companies store and process data globally. For instance, a U.S.-based cloud provider may be compelled to disclose data stored in European servers under American law, potentially conflicting with EU privacy regulations.

This extraterritoriality creates a legal minefield for businesses. They must navigate conflicting legal obligations, weighing the risk of non-compliance with one jurisdiction's laws against another. This scenario demands a heightened level of legal expertise and a strategic approach to data governance, urging businesses to be acutely aware of the legal landscapes of all countries in which they operate.

Dr. Avesta Hojjati, Head of R&D at DigiCert, underscores the complexity of data sovereignty requirements, stating that "each region has its own definition and requirements when it comes to data sovereignty." Ganesh Subramanya, Global Head – Data Security Practice, Cyber Security at Tata Consultancy Services, emphasizes the intricacy of global regulations as a primary challenge. "Global organizations operating in multiple jurisdictions face a complex web of local regulations to comply with every one of them." This diversity in regional requirements necessitates a nuanced approach to compliance, adding layers of complexity for businesses operating internationally.

"Global organizations operating in multiple jurisdictions face a complex web of local regulations making it quite difficult to manage compliance with every one of them."

Ganesh Subramanya
Global Head – Data Security Practice,
Cyber Security,
Tata Consultancy Services



"These countries have introduced rigorous data sovereignty and localization rules, forcing corporations to make decisions that may not be economically competitive or allow their citizens to participate in the global economy."

Kristin Lovejoy
Global Practice Leader,
Security & Resiliency, Kyndryl



However, the reality of data sovereignty is complex and often leads to multinational organizations opting out of certain markets due to increased costs and complexity associated with complying with data localization rules, underscores Kristin Lovejoy, Global Practice Leader for Security and Resiliency at Kyndryl. "Corporations are making decisions to take themselves out of certain markets, particularly emerging markets like the Middle East, Africa, and Southeast Asia. These countries have introduced rigorous data sovereignty and localization rules, forcing Western corporations to make decisions that may not be economically competitive or allow their citizens to participate in the global economy. This has led to an economic knock-on effect, potentially impacting GDP and expanding economic inequality."

Despite the legal challenges in interpreting these laws, Bruyere expresses concern that “these legal complexities often overshadow crucial topics like cyber resilience in cloud discussions.” Integrating legal compliance with cyber resilience strategies presents a significant challenge for businesses. On one hand, they must adhere to diverse and sometimes conflicting legal requirements regarding data storage and processing. On the other, they need to ensure that these compliance measures do not compromise their cyber resilience strategies.

Balancing Security, Usability and Data Governance

Ganesh Subramanya highlights the growing concern of data sprawl as organizations transition to multi-cloud environments. Ganesh confirms “the prevalence of data duplication as organizations transition to the cloud, driven by the desire to maintain data accessibility and security. Some applications remain on-premises, necessitating local data storage.” This process, often a precautionary measure, leads to an uncontrolled spread of data, creating further complexity in managing and securing it. Sébastien Cano, SVP Cloud Protection & Licensing at Thales, acknowledges that data sprawl is a fundamental issue for organizations, emphasizing the challenge of managing the increasing volume of data.

“Legal complexities often overshadow crucial topics like cyber resilience in cloud discussions.”

Agnieszka Bruyere

“The biggest challenge is how to implement data sovereignty in a way that is technically feasible and usable.”

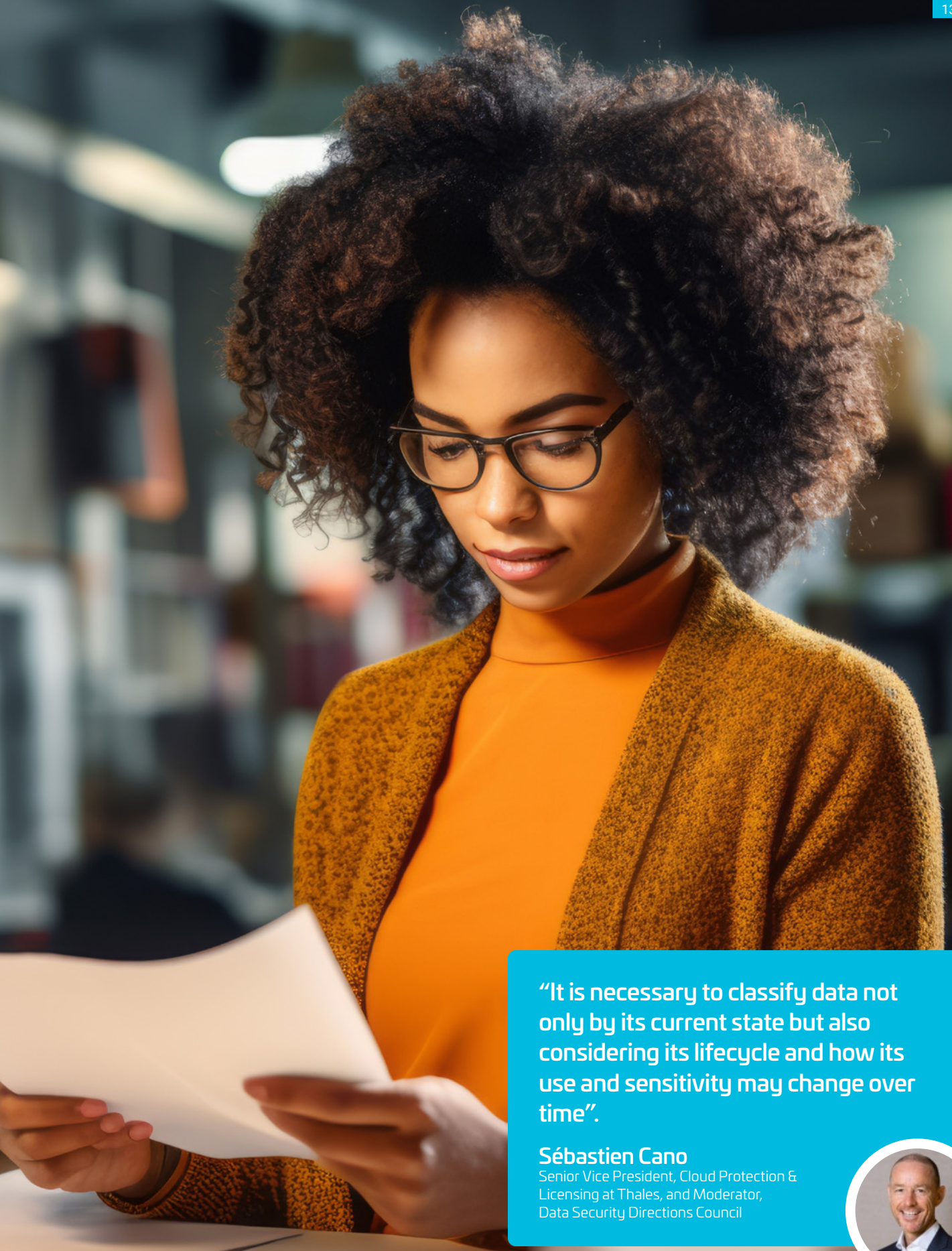
Dr. Avesta Hojjati
Head of R&D, DigiCert



This issue is exacerbated by a lack of proper data governance frameworks, making it difficult for organizations to understand and document data flows within their systems. Ganesh Subramanya underscores the challenge of balancing regulatory demands with operational needs. He highlights the need for “robust data governance frameworks to ensure visibility and control over data dispersed across multiple cloud environments.”

Furthermore, Dr. Avesta Hojjati discusses the tension between technical feasibility and practical usability in implementing data sovereignty, highlighting the need for solutions that are technically sound, yet user-friendly. “The biggest challenge is how to implement data sovereignty in a way that is technically feasible and usable.”

On the same topic, Michael Tadault, Chief Technologist Telco for APAC at Red Hat, stresses the ongoing struggle “to balance the need for tight security while enabling swift data access for agile business operations.” This is essential to transform security into an enabler for business growth rather than a barrier to innovation. However, it is important to note that although the privacy and security controls are always at odds with the business requirements, they are the ones that help build customer trust as highlighted in the latest Thales Consumer Digital Trust Index report.



“It is necessary to classify data not only by its current state but also considering its lifecycle and how its use and sensitivity may change over time”.

Sébastien Cano

Senior Vice President, Cloud Protection & Licensing at Thales, and Moderator, Data Security Directions Council



The Intricacies of Data Classification and the Need for Dynamic Governance

Data classification and dynamic governance are critical components in the management of information within organizations, especially in an era where data is both an asset and a liability.

Sébastien Cano addresses the critical task of setting sensitivity levels for data classification, acknowledging the challenges in determining the varying nature of data sensitivity. “The first thing you need to do is obviously define rules or set bars of data sensitivity.” However, identifying what data is highly sensitive versus what is not can be nuanced and challenging. Data varies greatly in sensitivity and regulatory burden. For instance, Personally Identifiable Information (PII), financial data, and health records require higher levels of protection due to privacy laws like GDPR or HIPAA. The challenge lies in accurately identifying and classifying this data amidst a vast pool of unstructured data.

Adding to the complexities above, the sensitivity of data can change over time. Data initially considered low-risk might become sensitive due to contextual changes, such as new regulatory requirements or changes in business operations. Sébastien Cano argues for a dynamic view of data governance, considering the lifecycle of data and its changing use and sensitivity. He emphasizes the need for continuous monitoring and protection of data, highlighting the overwhelming nature of this task for many organizations. “Several vendors are providing tools that offer a static view of the landscape. However, such a view is insufficient. A more dynamic view is required. It is necessary to classify data not only by its current state but also considering its lifecycle and how its use and sensitivity may change over time”.

SaaS Challenges and the Need for Agile Compliance Strategies

Chris Hickman, Chief Security Officer at Keyfactor, focuses on the “intricate challenges SaaS providers face in navigating different jurisdictional rules.” SaaS providers operate in a multifaceted legal environment where data sovereignty and privacy laws differ significantly across jurisdictions.

This complexity is heightened by the cloud-based nature of SaaS offerings, which often transcend national boundaries. SaaS providers must ensure their services comply with diverse regulations, which can vary in consent, data subject rights, and data breach notifications. The extraterritorial nature of some laws (like GDPR) can create jurisdictional overlaps, posing challenges for SaaS providers in determining which rules to follow when laws conflict.

“SaaS providers must closely collaborate with their customers to ensure tailored solutions that are compliant with regional laws.”

Chris Hickman
Chief Security Officer, Keyfactor



SaaS providers must balance the need for strict compliance with the operational efficiency of their services. Overly rigid compliance measures can impede user experience and service innovation. Chris Hickman advocates for a partnership between SaaS providers and customers to address legal complexities and foster trusted customer relationships. Says Hickman, “SaaS providers must closely collaborate with their customers. This partnership approach helps in understanding specific data sovereignty requirements and ensures tailored solutions compliant with regional laws.” Such collaborations not only aid in legal compliance but also “foster trust and reliability in customer relationships.”

Data Sovereignty Challenges: The Cloud Providers' Perspectives

Shifting Mindsets

In the evolving landscape of cloud computing, hyperscalers like AWS and Google Cloud are faced with the primary challenge of guiding users, especially those new to this realm, to understand and achieve data sovereignty within the cloud. Alex Meek-Holmes, Senior Manager of Sovereignty and Strategic Infrastructure in AWS, articulates this issue, pinpointing the prevalent reliance on outdated models of data security and management that are hardware-centric. He asserts, "The biggest challenge we see is in assisting our users to understand... how they can achieve data sovereignty whilst leveraging cloud services." This statement reflects the difficulties and challenges faced by organizations in shifting their mindset from conventional, on-premises infrastructures to more modern and flexible cloud-based paradigms. This transition involves a significant shift in the way people think about and approach technology, and it requires careful planning, strategy, and execution to ensure a successful outcome.

"The biggest challenge we see is in assisting our users to understand how they can achieve data sovereignty whilst leveraging cloud services."

Alex Meek-Holmes
Senior Manager of Sovereignty and Strategic Infrastructure, AWS



Transitioning from On-Premises to Cloud: Enhancing Security and Control

Meek-Holmes also highlights the critical transition from on-premises frameworks to cloud solutions, which involves overcoming barriers like excessive concerns over physical server access. He underlines the importance of this transition in bolstering security and control for clients, negating the misconception that cloud usage means compromising these elements. "Our biggest competitor is often described as on-premises IT. However, it is important for customers to understand that using the cloud does not mean compromising on security, resiliency, or control. In fact, by transitioning to the cloud, customers can achieve greater security, resiliency, and control."

Adaptability and Engagement

Contrasting, yet complementing Meek-Holmes' views, Brian Roddy, VP Engineering of Cloud Security at Google, places a strong emphasis on adaptability and engagement in addressing data sovereignty. He characterizes data sovereignty as a "moving target," which necessitates a flexible and evolving approach attuned to the varying global regulations. Google's strategy involves a proactive engagement with local regulators to build trust and ensure compliance. "We have to work with local regulators... to ensure we're meeting their expectations." He underscores Google Cloud's "substantial investment in data protection and transparency," aligning with these dynamic regulatory landscapes.

Balancing Cloud Benefits with Sovereignty Laws

Delving deeper, Roddy discusses the intricate balance between reaping the benefits of cloud services and adhering to data sovereignty laws. He believes that "context really matters," advocating for tailored organizational strategies in cloud adoption, considering factors like company size, location, and industry regulations. This approach is critical for scalability and considering long-term costs. "As the company grows, you want to be able to grow with it." Furthermore, Roddy addresses the complexity of international data exchange and the varying legislative requirements across countries. "Most enterprises have customers and partners in different countries. Business leaders must question when that data is exchanged; what is the implication of that? How do I secure that?"

Roddy's question sheds light on the intricate interplay that exists between the utilization of cloud technology and the adherence to various data sovereignty regulations that are often at odds with each other. The use of cloud technology has brought about a host of challenges for organizations, as data sovereignty regulations can differ significantly from one country to another, and even within regions of the same country. These regulations may require that data is stored and processed locally, which can make it difficult for organizations to take advantage of the benefits of cloud technology. As such, organizations must navigate this complex landscape carefully and ensure that they comply with all relevant regulations while still benefiting from the advantages of cloud technology.



Takeaways for Business Leaders


For business leaders across all sectors, this discussion offers crucial insights. It underscores the necessity of evolving from traditional data management models to embrace cloud computing while simultaneously navigating the complex waters of data sovereignty. This evolution requires a strategic balance of technological adoption, regulatory compliance, and proactive engagement with stakeholders and regulators. As cloud technology continues to advance, businesses must adapt their approaches to ensure they are not only reaping the benefits of the cloud but also adhering to the ever-changing landscape of data sovereignty laws and regulations.

“Data sovereignty is a moving target.”

Brian Roddy

Vice President Product Management,
Google



A man with a beard and glasses is shown in profile, looking intently at a computer monitor in a server room. The room is filled with server racks and glowing blue lights, creating a high-tech atmosphere. The man is wearing a dark jacket and has a focused expression. The background is slightly blurred, emphasizing the man and the monitor.

“It’s important to have a balanced approach to encryption, considering potential failure points and operational resilience.”

Agnieszka Bruyere

How do privacy regulations and data sovereignty requirements affect businesses' cloud strategies?

In the dynamic realm of cloud computing, data sovereignty stands as a critical factor shaping businesses' cloud strategies and operations. Data sovereignty mandates that data is stored, processed, and protected by the laws and regulations of the country or region where it resides. This intricate concept intersects with various aspects of cloud adoption, introducing complexities that businesses must astutely navigate.

The Ever-Evolving Legal Landscape

Experts from across the industry acknowledge the ever-evolving nature of data sovereignty regulations, posing challenges in comprehension and compliance. As Agnieszka Bruyere aptly says, "It's the complexity and the rhythm of new regulations. It's tough to embrace all these things: complexity, speed, and the broad subject." Tony Baudot addresses the complexity of regulations, saying, "The legal landscape is very much a moving target... new regulations are constantly being introduced."

This constant evolution necessitates consistent vigilance and agility in business strategies and a continuous learning cycle for businesses to stay abreast of the latest legal requirements and adapt their cloud strategies accordingly. A significant challenge is finding an equilibrium between data security and economic competitiveness. Tony Baudot states, "It's a bigger challenge... for data sovereignty because there are a lot of issues... legal compliance, data protection, business continuity."

"It's tough to embrace all these things: complexity, speed, and the broad subject."

Agnieszka Bruyere

In addition to the evolving legal landscape, data sovereignty regulations vary significantly across jurisdictions, creating a complex and fragmented legal landscape. This variability necessitates a thorough understanding of regional regulations and a willingness to adapt cloud strategies accordingly. Michael Tadault aptly observes, "The fragmented legal environment forces us to rethink our cloud strategy regularly."

"The fragmented legal environment forces us to rethink our cloud strategy regularly."

Michael Tadault
Chief Technologist for Telco
in APAC, Red Hat



Chris Hickman underscores the complexity of global data protection laws, emphasizing the need for a detailed understanding of regional differences. He observes, "While international laws like GDPR have common themes, regional differences require detailed understanding." This calls for a meticulous approach to legal compliance and a tailored strategy to account for these regional variations. The complexities of data sovereignty extend to the intricacies of cloud migrations and data classification. Chris Hickman underscores the importance of understanding not just the nature of the data but also its location: "Businesses need to be cognizant of where their data resides and how it is protected under different jurisdictions."

Localizing Operations to Align with Regulatory Frameworks

In a globalized business landscape, data sovereignty requires a tailored data management and security approach, particularly when operating across multiple jurisdictions. Dr. Avesta Hojjati emphasizes the need for localized operations: "You need to have a local presence... local teams, local data centers." This local presence allows for a deeper understanding of the unique legal and regulatory environments, enabling businesses to comply with local data sovereignty requirements effectively.

Each region... has its unique set of laws, culture, and way of doing business," asserts Dr. Hojjati. Companies must not only localize their physical and technological presence but also gain a deep understanding of the local laws, culture, and business practices to ensure successful operation within the framework of data sovereignty in different regions. "It's not just about having a local team, but also having your technology and services... adaptable to the local laws and regulations."

Alex Meek-Holmes presents a counterargument, emphasizing the high capital expenditure, scalability challenges, and security risks inherent in building localized data centers. "You need lots and lots of capital expenditure to get going... you need even more to have any kind of sense of being able to scale it," he points out, highlighting the significant financial investment required.

Adapting Cloud Strategies to Data Sovereignty Concerns

Businesses are increasingly reviewing their cloud deployments in response to data sovereignty concerns. Ganesh Subramanya highlights the delicate balance between cloud benefits and regulatory compliance: "There are concerns about moving to the cloud or improving existing cloud infrastructure. They are reviewing their cloud architectures and assessing existing data handling. Businesses seek guidance from cloud service providers, consultants, and system integrators to navigate this process." This highlights the need for a strategic approach that balances the efficiency gains of cloud adoption with data sovereignty considerations.

For those at the initial stages of cloud adoption, there is a heightened emphasis on due diligence, affecting timelines for cloud strategy implementation. Ganesh Subramanya conveys this trend: "They're doing much more due diligence now, even before pioneering using the strategy or defining how they will migrate data to the cloud."

Duncan Jones, Head of Cybersecurity at Quantinuum, discusses the significant effect of data sovereignty and privacy regulations on cloud deployment strategies. He cites the example of "defense contractors in the U.S. [who] have to comply with specific export control rules and data residency requirements." The emergence of government-specific cloud solutions, such as Microsoft's Government Community Cloud (GCC), demonstrates how the industry responds with tailored offerings to enable compliance and facilitate cloud adoption within regulated sectors.

The Emergence of Specialized Cloud Services

In response to these concerns, cloud providers are developing specialized services tailored to meet data sovereignty requirements. "We're seeing sovereign clouds being deployed across regions," underscores Ganesh Subramanya. Duncan Jones also notes the emergence of sovereign clouds, which "are designed to address the specific requirements of data residency and sovereignty." This tailored approach demonstrates the industry's commitment to enabling businesses to adopt cloud

technologies while adhering to stringent data sovereignty regulations.

Cloud service providers like Google, Microsoft, and AWS are expected to continue developing solutions and infrastructure supporting varied data sovereignty requirements worldwide. Duncan Jones notes the importance of "having tools to help businesses manage data sovereignty compliance, either provided by cloud services or developed in-house. This is necessary to prevent unauthorized data movement." These tools can automate processes, streamline compliance procedures, and reduce non-compliance risk.

On the other hand, Brian Roddy discusses the challenges and opportunities presented to cloud providers such as Google by restrictive data laws like those in France. He points out that while these regulations can be challenging in compliance, they also drive innovation in data management and protection strategies, benefiting businesses globally.

"It's not just about having a local team, but also having your technology and services adaptable to the local laws and regulations."

Dr. Avesta Hojjati

"Sovereign clouds are designed to address the specific requirements of data residency and sovereignty."

Duncan Jones

It's pushing us hard to make the right investments across the company." Investments prompted by restrictive legislation can yield widespread advantages: "[These] investments will help all around the world, even in less restrictive countries." This dual impact reflects the significant influence of data sovereignty laws on global tech and cybersecurity practices. Roddy conveys Google Cloud's proactive stance: "We view it as a core value of the cloud. That's why we're putting in such investment and want to provide optionality up to the highest standard possible."

The Financial Implications of Fragmented Legal Environments

Michael Tadault highlights the financial impact of navigating a maze of regulations, noting the increased operational costs and resources required to ensure compliance in each region. "This fragmentation inevitably leads to increased operational costs, as we need to deploy resources to ensure compliance in each region."

"SMEs, however, may face cost barriers due to regulations, which could be prohibitive. This is not the case for larger businesses that can afford to run multiple systems concurrently," underscores Duncan Jones. Businesses may need to operate dual systems to comply with regulations, adding complexity and potentially doubling the necessary infrastructure.

Data sovereignty laws also "affect decisions about data in transit and data at rest, shaping a company's cloud strategy and infrastructure requirements." Jones emphasizes "the fluid nature of cloud strategies," which must "adapt to business expansion and entry into new markets, each with their own data sovereignty challenges and associated costs." Jones advises on the necessity for "scalability" in cloud strategies to anticipate global expansion, suggesting businesses should proactively build flexibility into their cloud deployments.

The Foundations of Data Sovereignty: Strong Encryption and Effective Key Management

The Importance of Encryption to Data Sovereignty

In the complex and ever-evolving world of data protection, encryption stands as a beacon of security and control. For business leaders across both public and private sectors, understanding the nuances of encryption is not just a technical requirement but a strategic imperative. Encryption plays a multifaceted role in ensuring data sovereignty, a critical aspect of data governance that is increasingly coming under the scrutiny of regulatory bodies and security experts alike.

Encryption: A Bedrock for Data Sovereignty

Michael Tadault succinctly captures the essence of encryption in the realm of data sovereignty, stating, "Encryption is a key tool in ensuring data sovereignty. By encrypting data, we assert control over who can access it." This statement underscores the pivotal role encryption plays in ensuring individuals and organizations retain control over their data. "Data sovereignty is a crucial aspect of data protection, and encryption is a key component in ensuring compliance with this law," asserts Mark Hughes.

"Data sovereignty is pushing us to make the right investments across the company. We view it as a core value of the cloud."

Brian Roddy

Balancing Encryption, Compliance, and Operational Resilience

However, the path to effective encryption is not without its challenges. Encryption serves a dual purpose in the realm of data sovereignty. On one hand, it is a robust tool for safeguarding sensitive data against unauthorized access, thus playing a vital role in security strategies. On the other hand, it is also a compliance requirement in many jurisdictions.

However, encryption is only as good as its key management controls allow it to be. The control of the users, entities and applications that can access and use encrypted data is what will make or break the sovereignty program. As noted previously, data can't be locked away, it has to be used across the enterprise for competitive success, creating a balance between security and usability of data.

Agnieszka Bruyere underlines the importance of a balanced approach, advising "a balanced approach to encryption, considering potential failure points and operational resilience." To achieve this balanced approach, a "one-size-fits-all" solution rarely works in encryption. Oracle's nuanced strategy, offering clients various levels of encryption "from default encryption to the possibility to manage the keys with an external Hardware Security Module (HSM)," and allowing customers to choose "the right level of encryption based on data sensitivity," presents a blueprint for tailoring encryption to specific needs.

The Three Pillars of Data Encryption

Delving deeper into the operational aspects of encryption, businesses must consider three foundational factors:

1. Key generation: "I need to know that I generated it [the key] correctly."
2. Key distribution: "I need to know that I distributed it correctly."
3. Key usage: "I need to know that it's in use correctly."

Encryption is a critical aspect of maintaining the security and privacy of data in digital communications. To ensure the effectiveness of encryption strategies, it is essential to adopt a comprehensive approach. This approach should cover the entire process, from generating encryption keys to their correct distribution and usage. Poor key management can render even the strongest encryption algorithms ineffective. It also involves ensuring that keys are accessible to authorized personnel when needed, thus maintaining operational efficiency. This becomes even more complex in decentralized or cloud-based environments, where data and keys might be distributed across various locations and jurisdictions.

Future-Proofing Against Emerging Threats

Besides securing the foundations of data encryption, a forward-looking perspective on encryption is equally crucial. With NIST releasing the first set of encryption algorithms designed to withstand attacks from a quantum computer^{*}, system administrators must begin transitioning to the new standards as soon as possible, given that quantum computing advancements could render current encryption technologies obsolete. Most of where the business and personal data is living and moving will no longer be safe under current encryption technologies.

Businesses must begin to prepare for this future by staying informed about advancements in quantum computing and exploring PQC solutions. This forward-thinking approach is not just about maintaining security; it's also about ensuring that the business is agile enough to avoid any operational disruptions or compliance failures.

Navigating Global Encryption Standards and Regulatory Compliance

The international landscape of encryption standards adds another layer of complexity. Michael Tadault's observation that "Different countries have different encryption standards, which can be a hurdle in asserting data sovereignty across borders" highlights the challenges associated with varying global standards and international data transfers. Considering that data transfers are the bedrock of the global economy, what would be the impact if these transfers cannot be effectively safeguarded? The need for continuous alignment with diverse regulatory requirements compounds this concern. As Tadault further notes, "We need to ensure our encryption methods meet the regulatory requirements of each region we operate in."

The Delicate Balance Between Security and State Surveillance

Tadault also brings to light the tension between encryption for data security and government policies. His statement, "However, we're seeing more governments pushing for backdoors in encryption, which undermines its effectiveness," points to the ongoing debate and delicate balance between using encryption as a defense against unwarranted state surveillance and respecting legitimate state concerns for national security.

In conclusion, data sovereignty, an essential facet of data protection, is deeply intertwined with the strategic application of encryption. Business leaders must navigate the complexities of encryption, from operational resilience to compliance with international standards, all while keeping an eye on future technological shifts. The careful balance between ensuring robust encryption for data control and responding to evolving regulatory and security landscapes is not just a technical challenge but a strategic imperative in the modern digital world.

^{*}<https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>



“It doesn’t matter where your data is.
It is who controls the keys.”

Brian Roddy

The Importance of Key Management to Controlling Your Data

In an era where data is the new gold, controlling it is paramount for business leaders across both public and private sectors. Central to this control is the concept of key management in data encryption; a critical pillar in maintaining data sovereignty.

The Fundamental Principle of Cryptography

To begin with our analysis of the topic, it is essential to remember the foundation of encryption; while cryptographic algorithms are public, the associated keys must remain secret. The algorithms are well established, and everyone can use the same algorithm. The encryption key is the secret parameter to data protection. This principle highlights the crucial role of key management: the best systems are vulnerable if the keys are not adequately protected.

“We want to make sure that our clients understand what their responsibility is.”

Agnieszka Bruyere

Understanding Client Control in Key Management

The first aspect of effective key management is client awareness and understanding. Agnieszka Bruyere, emphasizes this, underscoring Oracle’s commitment to client awareness, especially when using advanced options like external HSMs. “We really want to make sure that our clients understand what their responsibility is,” Bruyere states. This focus on client education and empowerment is not just about compliance but about enabling clients to make informed decisions, ensuring that key management practices are both effective and secure.

Technical Solutions and the Evolution of Data Sovereignty

Traditionally, the focus of encryption has been on data at rest. However, Brian Roddy’s insights signal a paradigm shift towards a more holistic approach. “How do you make sure data is encrypted not only when at rest but in processing, including confidential support inside of Graphics Processing Units (GPUs)?” Encrypting data in transit and, crucially, during processing, particularly in environments like GPUs, represents a significant advancement. This shift is crucial as it acknowledges the dynamic nature of data usage in modern businesses, where data is continuously accessed, processed, and shared. The implication for business leaders is clear: data sovereignty now requires a multi-faceted encryption strategy that protects data across all stages of its lifecycle.

Roddy also underscores a shift in focus from the physical location of data to the control over encryption keys. “It doesn’t matter where your data is. It is who controls the keys.” The evolution of data sovereignty is closely linked to the control over encryption keys. “It’s our belief that if the customer controls the keys... that data is safe and protected,” explains Roddy.

His emphasis on customer control over these keys underpins the notion that data sovereignty extends beyond mere possession (and storage) of data. It’s about having the authority and means to control access and usage. This development is particularly relevant in scenarios involving cross-border data transfers and international regulations. Businesses must now ensure that their data governance policies are robust enough to handle the complexities introduced by varying jurisdictional requirements, all while maintaining control over their encryption keys.

The Complexities of Multi-Cloud Environments

The rise of cloud and multi-cloud environments has added another layer of complexity to data sovereignty. With data dispersed across various cloud platforms, each with its own set of controls and security measures, the task of maintaining sovereignty becomes more challenging. This dispersal of data and encryption keys across multiple platforms complicates key management. Yet, as regulatory requirements evolve, the control of data – and, by extension, the encryption keys – becomes paramount.

This dispersion necessitates a unified approach to key management across platforms. Business leaders must now consider solutions that offer centralized control over keys, regardless of where the data resides. Ganesh Subramanya rightly notes, “The best way to control [your keys and data] is to assert control over the encryption keys themselves.” This approach not only simplifies key management but also ensures consistent application of security policies across different environments, which is essential in a fragmented cloud environment.

Ownership and Management of Keys

The ownership and management of encryption keys are central to the concept of data sovereignty, particularly in our increasingly digital world. Ownership of encryption keys is more than a matter of possession; it’s a statement of controlling management and access to build trust. When an organization owns its encryption keys, it retains control over its data. This control translates into the ability to decide who accesses the data and under what circumstances. However, with ownership comes the responsibility of managing these keys securely, which leads to the need for robust key management practices.

“The best way to control your keys and data is to assert control over the encryption keys themselves.”

Ganesh Subramanya

Effective key management practices are the backbone of maintaining data sovereignty. The challenge in key management often lies in balancing convenience with security. Sébastien Cano points out the pivotal role of key management in sovereign cloud projects. “One of the key questions always is how encryption is managed. The key management infrastructure is essential to ensure proper control over the encryption mechanism.” While stringent security measures are essential, they should not impede the operational efficiency of the organization. Solutions like HSMs offer a balance by providing high security for key management while maintaining operational efficiency.

“One of the key questions always is how encryption is managed. The key management infrastructure is essential to ensure proper control over the encryption mechanism.”

Sébastien Cano

Selecting the Appropriate Key Management Approach

The strategic management of encryption keys is central to data sovereignty, serving not just as a technical necessity but as a cornerstone in the broader discussion of data control and security. Our experts delve into the available key management approaches, namely Bring Your Own Keys (BYOK), Hold Your Own Key

(HYOK), and Bring Your Own Encryption (BYOE), offering insights and analysis to guide business leaders in making informed decisions aligned with their specific security and sovereignty needs.

The Debate Over Key Management Strategies and Data Sensitivity

The discourse surrounding key management strategies in the context of data sensitivity is increasingly becoming a focal point for organizations striving to balance data sovereignty and security. This debate encompasses a spectrum of strategies, from autonomous key management, to high-watermark approaches in data protection, as well as the nuanced consideration of tailoring key management to the sensitivity of data.

The move towards autonomous key management strategies like BYOK, HYOK, and BYOE represents a growing trend among organizations seeking greater control over their data. These methods afford organizations the ability to exercise sovereignty over their encryption keys, thereby exerting more control over their data, even when it resides in cloud environments.

- BYOK offers a balance, allowing organizations to generate keys in their environment and import them into the cloud. However, as Ganesh Subramanya comments, “While this gives some control, it still leaves the keys under the cloud provider’s umbrella to a certain extent.”
- HYOK takes this a step further, says Ganesh Subramanya, by ensuring that “keys are stored within the organization’s domain, not the cloud provider’s, offering greater control.”
- Finally, BYOE is considered the most secure and complex, involving the use of an organization’s own cryptographic libraries at the application layer. This is considered the most challenging approach,” notes Ganesh Subramanya, “but is the most suitable for highly sensitive data where maximum security is paramount.”

The high-watermark approach to data protection simplifies data protection management and reduces errors, especially in environments where data of varying sensitivities is intermixed. This approach entails securing all data at the level required for the most sensitive, mitigating the complexity of managing different cryptographic standards. Such an approach is particularly beneficial in cloud computing contexts where data aggregation increases the risk of mismanagement and exposure.

When business data is intermixed, managing different algorithms and different keys adds complexity. What businesses have to do is look at the data, determine the most sensitive one, and establish the strongest security for this data. Then, protect all the business data at that higher level. Businesses want to do a higher watermark data protection; otherwise, the management becomes too complicated and mistakes can be made.

“A hybrid model using both on-premises and cloud-based key management offers flexibility and meets diverse needs.”

Michael Tadault

A different approach, suggested by Michael Tadault and Sébastien Cano, is adopting a hybrid model, blending on-premises and cloud-based key management solutions. The hybrid model offers a pragmatic approach that aligns with the varying sensitivities of data. This model acknowledges that not all data is created equal and that the level of protection should correspond to the level of sensitivity.

- For highly sensitive data, organizations might prefer on-premises key management, retaining physical control over encryption keys for a higher security level.
- Less critical data, conversely, can leverage cloud-based key management services, benefiting from their flexibility and scalability.

Tadault states, “We prefer on-premises key management for our most sensitive data. For less critical data, we use cloud-based key management services for their flexibility and scalability.” Sébastien Cano also emphasized the importance of tailoring key management strategies to the level of data sensitivity, highlighting that “Some methods are more complex and suitable for more sensitive data. They should be associated with the level of sensitivity of the data.”

This hybrid approach ensures that organizations don’t adopt a one-size-fits-all strategy but rather a tailored solution that offers the optimal balance between security, flexibility, and practicality. In Tadault’s words, “A hybrid model using both on-premises and cloud-based key management offers flexibility and meets diverse needs.”

Centralizing encryption key management is recommended as a best practice, even as companies struggle with key management across various cloud and SaaS offerings. “Having a central repository for all your encryption keys is definitely a best practice that all companies should do”, Sébastien Cano states, as well as illustrating the difficulties of managing encryption keys across numerous services. “You start having keys all over the place and that becomes unmanageable very quickly.” Cano uses a metaphor to convey the need for simplicity and security in key management, drawing a parallel to having a manageable keychain in everyday life. “You don’t want keys to be all over the house... you put an Apple air tag on it, so you know where it is all the time.”

Cano describes the push for external key management as a means of ensuring data sovereignty, allowing customers to retain control over their encryption keys. “[Thales] has been the ones really promoting this concept of an external key management for the cloud encryption.” Cano emphasizes that while encryption is foundational for complying with various regulations, its efficacy is contingent upon proper key management. “One of the best ways to enforce privacy and enforcing the protection of data is to be encrypted. Maintaining control over encryption keys, which in turn ensures control over the data irrespective of its geographical location, is crucial. Customers will want to remain in control of their encryption keys”

“Maintaining control over encryption keys, which in turn ensures control over the data irrespective of its geographical location, is crucial.”

Sébastien Cano

“Any chosen solution must be flexible enough to accommodate upcoming changes due to evolving data sovereignty requirements.”

Dr. Avesta Hojjati

Dr. Avesta Hojjati underscores the importance of adaptability in choosing the optimal key management approach. He stresses that “any chosen solution must be flexible enough to accommodate upcoming changes due to evolving data sovereignty requirements.” This adaptability is not just a technical requirement but a strategic imperative for organizations navigating the complexities surrounding data sovereignty, including regulatory changes, technological advancements, multi-cloud environments, and evolving cybersecurity threats.

However, before even considering which key management solution to select, businesses should perform their due diligence. Ganesh Subramanya and Duncan Jones both advise a risk-based approach in selecting key management strategies. Integrating these strategies into a holistic approach to data security involves a careful assessment of the organization’s specific needs, regulatory requirements, and the sensitivity of the data in question. The decision-making process should consider:

- Risk Assessment: Evaluating the risks associated with different types of data and choosing the appropriate key management strategy accordingly.
- Regulatory Compliance: Ensuring that the chosen strategy aligns with relevant data protection laws and industry regulations.
- Technical Capabilities: Assessing the organization’s technical capacity to implement and manage these key management solutions effectively.
- Cost-Benefit Analysis: Weighing the costs of implementing a particular strategy against the benefits of enhanced security and control.

The Impact of Emerging Technologies on Data Sovereignty: Quantum Computing, 5G, and AI

The Impact of Quantum Computing

Quantum computing is set to revolutionize a myriad of fields, including medical, manufacturing, and finance. Its capacity to handle multi-dimensional interactions and relationships opens the door to more complex solutions, mirroring natural, as well as business processes, like photosynthesis, engineering, and actuarial predictions. This innovation is a pivotal tool in understanding intricate processes.

However, the advent of quantum computing brings significant implications for data protection. It is also going to enable crypto analysis, which is going to break some of the existing algorithms that we know today, specifically against Shor's algorithm.⁴

While the full impact of quantum computing may still be on the horizon, its potential threat to encryption is being seriously considered. Sébastien Cano warns, "The quantum battle has already started... Harvesting attacks are happening right now." This futuristic combat between cryptographic strength and analysis, is an ongoing race.

The relentless technological progression, akin to Moore's Law, is constantly eroding the frontiers of cryptography, necessitating perpetual evolution. Looking at the topic from a historic view, it was always a race between the cryptographic strength of a specific algorithm or the size of a specific key compared to what is available from a cryptanalysis perspective.

While Duncan Jones acknowledges that "data sovereignty is a challenging part of the question" when it comes to quantum computing, Dr. Avesta Hojjati brings the discussion to the core issue of data sovereignty. At the heart of data sovereignty lies the ability to protect and control access to data. Traditional encryption methods, the bedrock of current cybersecurity protocols, are potentially vulnerable to quantum computing's capabilities. Quantum computers, with their ability to perform complex calculations at unprecedented speeds, could eventually render existing cryptographic algorithms obsolete. This looming threat to encryption standards like RSA is a pressing concern for data sovereignty, as it directly impacts the ability of nations and organizations to safeguard sensitive information.

"We need to start thinking about post-quantum cryptography today."

Dr. Avesta Hojjati

"The quantum battle has already started... Harvesting attacks are happening right now."

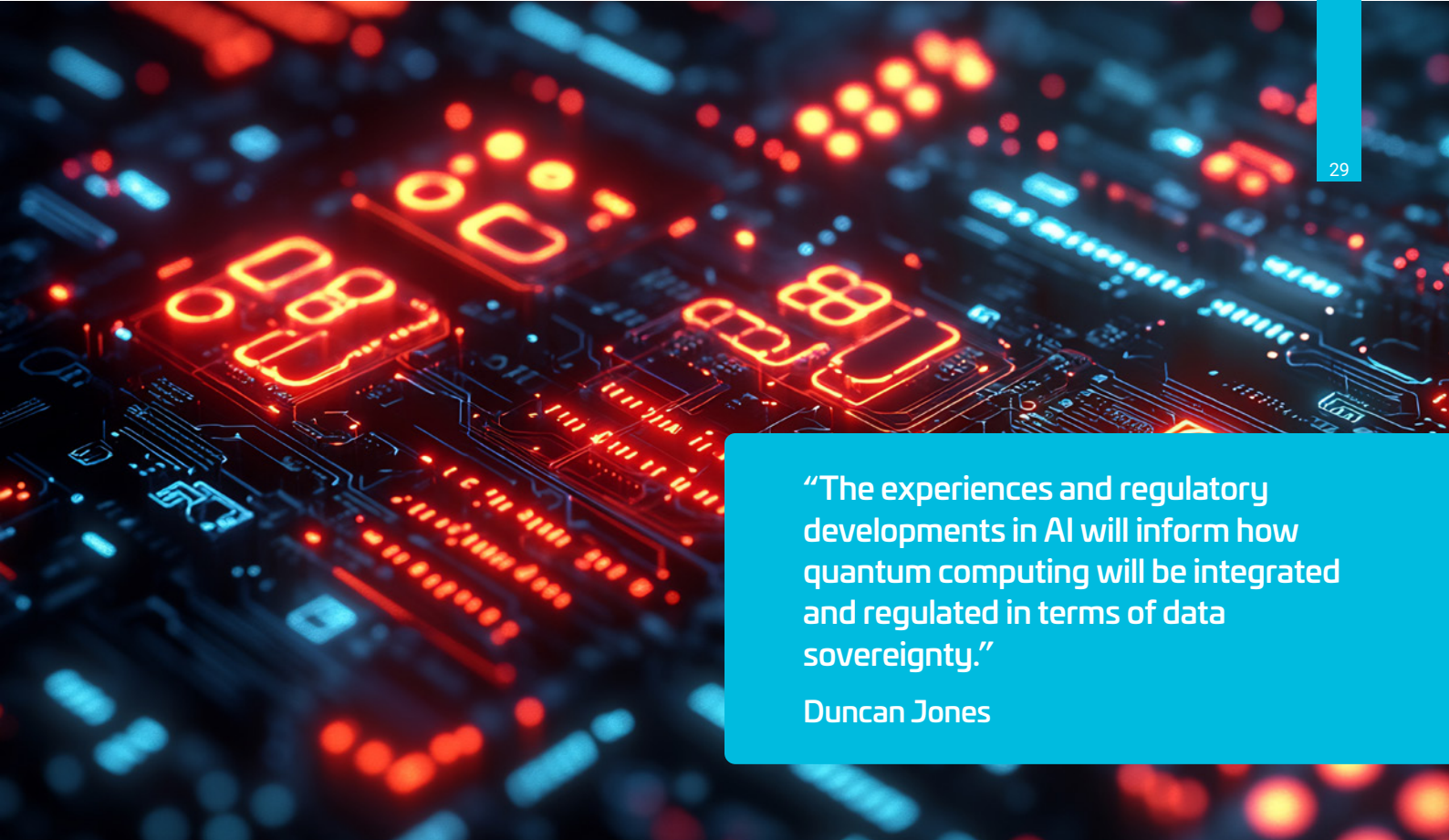
Sébastien Cano

"Harvest Now, Decrypt Later"

The strategy of "harvest now, decrypt later" employed by adversaries poses a significant and strategic threat to data sovereignty. This approach involves collecting encrypted data with the intention of decrypting it in the future using quantum computers. This tactic highlights a critical aspect of data sovereignty – the need for long-term security. Data that is encrypted today must remain secure for many years, as future advancements in quantum computing could enable retroactive decryption of historical data.

Dr. Hojjati places emphasis on the need for proactive adaptation in cryptographic technologies reiterating the urgency for developing and implementing post-quantum solutions. "We need to start thinking about post-quantum cryptography today," urges Dr. Avesta Hojjati. This shift requires not just technological innovation but also a paradigm change in how organizations approach data security. Proactive adaptation in cryptographic strategies is imperative to safeguard data against the advanced capabilities of quantum computing.

⁴<https://plato.stanford.edu/entries/qt-quantcomp/>



“The experiences and regulatory developments in AI will inform how quantum computing will be integrated and regulated in terms of data sovereignty.”

Duncan Jones

Post-Quantum Cryptography and Crypto Agility

With NIST publishing the principal set of quantum-safe cryptographic algorithms, the concept of crypto agility emerges as a strategic response to the evolving threats of quantum computers, underscores Sébastien Cano. Crypto agility becomes more crucial as “some quantum-resistant algorithms already exist and are available today,” explains Cano.

Besides the known security challenges that compound quantum computing, Duncan Jones sheds light on the data sovereignty concerns that encompass “not just the data itself but also the geographical location of quantum computing resources.” As a result, Duncan Jones forecasts a potential shift towards localized quantum computing, driven by the need for data sovereignty, albeit accompanied by challenges “such as specialized workforce requirements and significant investments.”

On the same topic, advancements in post-quantum cryptography will most likely elevate the conversation about digital privacy and protection, particularly concerning the risks of current encryption methods becoming obsolete with the advent of quantum computing. Security professionals believe that controls like homomorphic encryption, data confidentiality, and confidential computing, together with new protection mechanisms based on physics rather than mathematics, will be the future.

Finally, and considering the legislative initiatives in the AI realm, such as the EU AI Act, Duncan Jones believes that “the experiences and regulatory developments in AI will inform how quantum computing will be integrated and regulated in terms of data sovereignty.” He thinks that “the AI industry’s regulatory journey can help learn from the data when it comes to quantum computing.”

As the impact of quantum computing on data sovereignty extends beyond technology into the realms of governance and policy, governments and international bodies need to consider how quantum computing could affect broader issues such as national security, international relations, and economic competitiveness. Policies and regulations need to be agile and forward-thinking to keep pace with technological advancements, ensuring that data sovereignty is maintained in a rapidly evolving digital landscape.



The Impact of 5G Technology

The advent of 5G technology has ushered in a new era of digital communication, marked by enhanced bandwidth and spectrum efficiency. This evolution, primarily seen in the transition from 5G to 6G standards, has led to a significant increase in IP addresses, optimizing bandwidth usage and spectrum efficiency. This technological leap forward addresses the consumer's ever-growing demand for improved bandwidth and connectivity, enabling more sophisticated activities on smartphones.

However, this progression is not without its challenges. As the network capabilities expand, so does the complexity of managing privacy and data sovereignty. Mark Hughes raises an important point in this context. He notes, "Network operators now need to be more intrusive to maximize the use of available bandwidth, potentially leading to more data collection about the devices themselves." This statement underscores a pivotal dilemma in the 5G era: the balance between network optimization and individual privacy.

5G technology is not merely an incremental upgrade in network capabilities; it is a transformative shift that redefines how and where data is processed and stored. Unlike its predecessors, 5G's architecture inherently supports the decentralization of data processing, moving it closer to the data source, a concept known as edge computing. This shift from centralized cloud-based data centers, to localized computing resources is significant for several reasons:

Firstly, localizing compute resources dramatically reduces latency, a critical requirement for applications to operate more efficiently and reliably. Secondly, and more pertinently to Meek-Holmes' point, is the aspect of digital sovereignty. With data increasingly being processed at the local level, countries have greater control over the data generated and processed within their borders. This control is crucial in an era where data is a strategic asset, and its management is subject to national laws and regulations. The ability for 5G cores to operate within national borders addresses a growing concern among countries about data being stored and processed in foreign territories, subject to different legal and regulatory frameworks.

However, this shift also poses challenges. The emphasis on digital sovereignty raises concerns about the "balkanization" of the internet, where the global, open nature of the network could shatter into a patchwork of regional internets, each with its own rules and standards. This fragmentation could hinder the seamless global exchange of information, impacting businesses, especially those operating internationally, and potentially slowing down the pace of innovation. For more insights on this topic, see the respective section on internet fragmentation.



“5G is going to make the problem of data sprawling grow even faster.”

Sébastien Cano

Data Volume and Edge Computing

The conversation on data sovereignty in the 5G era is incomplete without discussing the dramatic increase in data volume and mobility, as highlighted by Michael Tadault. “5G dramatically increases the amount of data generated and its movement.” 5G’s high-speed connectivity and lower latency means that significantly more data can be generated, transmitted, and processed at unprecedented speeds.

The increased mobility of data complicates the control and enforcement of data residency laws and regulatory compliance. With data flowing across borders more fluidly, ensuring that data handling adheres to the varying regulations of different jurisdictions becomes more complex. This complexity is exacerbated when considering the global nature of many 5G-enabled services and applications, which may not align neatly with national regulations.

Sébastien Cano echoes similar sentiments, emphasizing the accelerated need for advanced cybersecurity measures due to the increase in data volume and complexity in security management. “5G is going to make the problem of data sprawl grow even faster.” The emergence of edge computing, a key feature in 5G networks, further intensifies these challenges. As Sébastien Cano points out, edge computing processes more data outside centralized control, leading to a decentralization of data management. This decentralization can make it harder for Chief Security Officers to enforce consistent security protocols, as data is processed and stored in multiple, often geographically dispersed locations.

Given these challenges, the call for advanced cybersecurity measures is both timely and critical. Traditional security frameworks may not be sufficient in this new landscape. Michael Tadault rightly points out the complexities arising from this surge in data flow and speed. “This makes controlling where our data resides and ensuring compliance more complex.” As Tadault suggests, the need to implement advanced security measures is not just about enhancing existing protocols, but also about innovating new methods to secure data in transit and at rest, especially in decentralized environments.

Businesses and policymakers must adapt to these changes by developing more robust and flexible security strategies. To address these challenges, specific solutions for encrypting data in 5G networks are being developed, focusing on container encryption due to the architecture of 5G deployment. As Sébastien Cano states, “Thales has developed specific solutions to encrypt containers and protect information that is in containerized infrastructures.” This initiative demonstrates the proactive approach to adapting encryption technologies to the evolving needs of 5G networks.



The Impact of Generative AI

In the rapidly evolving world of Artificial Intelligence (AI), the concept of data sovereignty has become increasingly complex. The focus on confidentiality, particularly in the context of generative AI, is crucial as these tools pose unique challenges in terms of data privacy and security. Emphasis should be placed on the importance of protecting personal data used in training AI models. So far, the training data has contained sensitive or proprietary information, making its protection paramount.

“The question of data utilization and who is responsible for training the AI models is very important.”

Agnieszka Bruyere

Ethical and Legal Implications

The ethical and legal implications of data utilization in AI are complex. Agnieszka Bruyere’s pronouncement, “The question of data utilization and who is responsible for training the AI models is very important,” brings to light a key concern in the AI field. Who holds the responsibility for ensuring that the data is used ethically and legally? This responsibility traditionally lies with the organizations developing AI, but as AI becomes more pervasive, this responsibility could extend to third-party data providers, regulatory bodies, and even end-users.

By advocating for the use of private data in a controlled and secure manner, Bruyere points out a sustainable path forward. This approach allows businesses to harness the power of generative AI without compromising the confidentiality and sovereignty of client data. It necessitates robust data governance frameworks, where data privacy is not an afterthought but a foundational aspect of AI model development.

The overarching theme, according to Bruyere, is the harmonization of data sovereignty with business value. Bruyere rightly points out that the value derived from AI must not compromise data sovereignty. This stance is both ethically sound and also strategically prudent in a global business environment increasingly concerned with data privacy and security. Businesses leveraging AI must navigate a complex web of regulations and ethical considerations to maintain consumer trust and legal compliance.



Regulatory Challenges in the Age of AI

Tony Baudot's observation that "Technological advancements are both a blessing and a curse in the context of data sovereignty" captures the essence of the double-edged nature of modern technology. On one hand, advancements in AI and related technologies have brought unparalleled efficiencies in data management and security. These technologies enable the processing and analysis of large datasets, offering insights that were previously unattainable. This aspect of technology can be seen as a blessing as it drives innovation, streamlines operations, and enhances decision-making processes.

However, on the other hand, the curse that Baudot refers to is equally significant. The rapid pace of technological change often outstrips the development of appropriate governance structures and ethical guidelines. This lag creates a vacuum where data can be misused or mishandled, leading to breaches of privacy and violations of data sovereignty. The challenge here is to establish a balance – leveraging the benefits of technological advancements while simultaneously protecting the rights and privacy of individuals and organizations.

Although the enforcement of the EU AI Act and other global regulatory initiatives are great steps toward responsible AI, the truth is that the velocity of the evolution of technology greatly outpaces the evolution of regulatory controls. The rapid development of

AI-powered threats like DeepFakes has outstripped existing legal and regulatory frameworks. The ability to generate realistic content raises significant issues regarding digital rights and data ownership. The majority of current legal frameworks were developed in a pre-AI era and thus are often ill-equipped to handle the nuanced challenges presented by AI-generated content.

This discrepancy leads to a legal grey area, where existing laws do not fully cover activities and their consequences, leaving individuals and organizations vulnerable to exploitation and misuse of their data. Governments have begun to realize the need for more agile and robust regulatory mechanisms that can adapt to technological advancements and adequately protect data rights and sovereignty.

"Technological advancements are both a blessing and a curse in the context of data sovereignty."

Tony Baudot

Regulate and Innovate: How Legislation Drives Technology Innovation

Regulatory Challenges as an Opportunity for Innovation

In the complex landscape of data sovereignty, regulatory challenges are often perceived as obstacles. However, an emerging school of thought suggests these challenges could be the catalyst for a new wave of innovation, especially in the realms of technology and business strategy.

Data sovereignty is not just a matter of implementing the right technology; it's about integrating technological solutions with comprehensive contractual frameworks. As Agnieszka Bruyere insightfully notes, the synergy between technology and legal frameworks is critical. "Both technology and a contractual

framework are needed to make it work. It's not just about having the right technology." This perspective demands a shift in how organizations approach data sovereignty – it is no longer sufficient to focus on technical compliance alone. Companies must ensure that their technological advancements align with evolving legal standards and contractual obligations, ensuring a cohesive strategy that addresses all facets of data sovereignty.

"Technology, policy and a contractual framework are needed to make it work. It's not just about having the right technology."

Agnieszka Bruyere

A Catalyst for Technology Innovation

Furthermore, Ganesh Subramanya's insights underscore the paradoxical nature of data sovereignty; while it may impose restrictions on data sharing and challenge innovation, these very limitations can catalyze the development of novel solutions. According to Ganesh Subramanya, data sovereignty "spurs the development of new solutions."

This scenario exemplifies the classic principle that necessity is the mother of invention. The restrictions imposed by data sovereignty compel companies to think creatively, leading to the development of innovative technologies and methodologies for data management and compliance. This situation presents unique opportunities for businesses to differentiate themselves by offering new solutions that address these specific challenges.

The impact of data sovereignty on sustainability is an emerging area of concern and innovation. The requirement for local data storage and the risk of data duplication carry significant environmental implications. Ganesh Subramanya's perspective highlights an opportunity within this challenge, that is, the development of green technologies and sustainable practices in data management. This approach is not just about compliance with regulatory standards but also about contributing to a more sustainable and environmentally responsible business model. By focusing on sustainability, companies can not only meet regulatory requirements but also enhance their corporate social responsibility profiles and appeal to increasingly eco-conscious stakeholders and consumers.

Duncan Jones echoes this sentiment, viewing "data sovereignty not just as a compliance issue but as an opportunity for technological advancement." This viewpoint brings a strategic dimension to the conversation, emphasizing the need for businesses to manage the costs associated with innovation in response to data sovereignty. It further necessitates a balance between investing in new technologies and maintaining cost-effectiveness. Jones's perspective suggests that innovation in response to data sovereignty is not just a technical challenge but also a financial and strategic one. By optimizing processes and developing cost-effective solutions, companies can turn the compliance cost into an investment in future capabilities and market differentiation.

Duncan Jones and Tadault both highlight the potential for proactive problem-solving in the realm of data sovereignty and privacy. Tadault, in particular, points out that "these regulations can push companies towards more proactive security measures." At the same time, Jones suggests that "innovation can help in optimizing and making the process more efficient in meeting data sovereignty requirements." As such, "new technological solutions will likely emerge to drive efficiency in meeting data sovereignty requirements."

This shift can lead to the development of advanced security strategies and technologies, which are crucial in today's digital landscape. The emphasis on proactive security measures not only ensures compliance but also enhances the overall security posture of organizations, making them more resilient against cyber threats.



Transforming Business Culture Through Data Responsibility

Lastly, Tadault touches upon the broader cultural impact of these regulations. He observes, “It’s also transforming business culture to be more data-responsible, which I believe is essential for long-term success.” Tadault’s observation sheds light on a pivotal cultural shift in the corporate sphere – the move towards a more data-responsible ethos. This shift is not merely a reaction to the stringent legal requirements of data sovereignty, but reflects a deeper, more ethical approach to handling data. In today’s digital age, data is an invaluable asset, and how organizations manage this asset speaks volumes about their corporate integrity and values. Data responsibility encompasses aspects like privacy, security, and ethical usage, which are becoming key determinants of an organization’s reputation and trustworthiness.

Data sovereignty laws are compelling businesses to reevaluate their data management practices, placing an increased emphasis on ethical considerations. This evolution goes beyond compliance; it’s about embedding a sense of responsibility in every action involving data. Companies are now expected to handle data not just legally, but ethically, fostering trust among customers, partners, and regulators. This ethical dimension of data management is rapidly becoming a benchmark for evaluating corporate integrity and social responsibility. In a world where data breaches and misuse of data are increasingly under public scrutiny, adopting a data-responsible culture is not only a regulatory necessity but a moral imperative.

“It’s also transforming business culture to be more data-responsible, which I believe is essential for long-term success.”

Michael Tadault

The push towards data responsibility is also driving innovation in data management practices. Businesses are exploring new technologies and methodologies to ensure data privacy and security while maintaining operational efficiency. This includes the development of more robust data encryption techniques, secure data storage solutions, and innovative data processing algorithms that respect user privacy.

The Rise of Privacy-Enhancing Technologies (PETs)

Dr. Avesta Hojjati emphasizes the surge in PET-related activities and developments: “PET is one of the biggest areas that [data sovereignty] is going to expose on. In the past 24 months... every quarter there is a PET conference,” and “a PET technology as a product that is coming out.” This trend highlights an accelerated pace of innovation in PETs, spurred by the growing need to address data sovereignty concerns. PETs are rapidly becoming a cornerstone in the tech landscape, offering novel ways to handle data while respecting privacy and legal boundaries.

Brian Roddy illustrates this trend by discussing Google’s initiative on “confidential spaces” aimed at preserving user privacy in the face of phasing out third-party cookies. He highlights the significance of technologies like secure multi-party computation, noting, “that’s an area we’re investing more and more in.” Roddy’s insights underline the potential of PETs not only in enhancing privacy but also in enabling international data sharing in compliance with data sovereignty laws.

The journey of homomorphic encryption, a key PET, is particularly illustrative. Initially conceptualized over two decades ago, it has evolved from a theoretical idea to a practical tool. However, despite its evolution, NIST has not approved homomorphic encryption algorithms. This highlights a critical point: while PETs like homomorphic encryption are promising, they must navigate a complex landscape of regulatory compliance and technical validation.

It is also essential to stress the importance of investing in PETs as complementary tools rather than replacements for existing cryptographic practices. PETs can act as compensating controls in scenarios where traditional methods are not viable, thereby offering businesses a flexible approach to data security and compliance.

Fully Homomorphic Encryption (FHE) is a very promising technology and foundational in addressing data sovereignty challenges. Although not fully matured, FHE is a very good answer to data sovereignty, just like confidential computing, multi-party computing, and enclave computing. On top, FHE is a very commercializable technology that can potentially resolve the cloud computing conundrum related to data sovereignty.



“PET is one of the biggest areas that data sovereignty will expose on.”

Dr. Avesta Hojjati

Strategic Insights: Internet Balkanization, Cyber Warfare, and The Future of Data Transfers

Internet Balkanization: A Credible Risk?

In the rapidly evolving digital age, the concept of internet balkanization, or fragmentation, has emerged as a crucial concern for business leaders, technologists, and policymakers. Agnieszka Bruyere, observing the evolving landscape, notes the potential for internet fragmentation due to varying frameworks, rules, and certifications across geographies. However, this business environment illustrates the delicate balance between the perceived safety of sovereign clouds and the desire for a seamless global experience, particularly for international companies.

Adding to this, Hickman warns about the potential for a “fragmented internet” due to varying data sovereignty laws accelerated by technological advancements. This fragmentation could arise as “nations develop their own data protection standards in response to the advanced capabilities of quantum computing and 5G.” The of EU AI Act is a fine example of this concern.

However, there are also ongoing regulatory efforts that acknowledge the need for cross-border data transfer, such as the Data Privacy Framework between the US and EU. Ganesh Subramanya acknowledges that “The governments and regulators have understood there is a real need, and we can’t really isolate everything and grow like that.”

“Fragmentation could arise as nations develop their own data protection standards in response to the advanced capabilities of quantum computing and 5G.”

Chris Hickman

Michael Tadault brings a different perspective to the discussion, stating, “Internet fragmentation is undoubtedly a political issue.” He notes the role of sovereign internet policies in contributing to fragmentation, often driven by political agendas. “Countries exerting more control over their segment of the internet, often for political reasons, is a major contributor to this fragmentation.”


“Countries exerting more control over their segment of the internet, often for political reasons, is a major contributor to this fragmentation.”

Michael Tadault

However, the inefficiencies brought about by a fragmented internet may deter this risk from becoming a reality. “The benefits of globalization are that it promotes specialization and interdependence, leading to mutual gains. If everybody is trying to do the same thing, it’s also not economically sustainable on the macro-economic level,” argues Michael Tadault.

Finally, Kristin Lovejoy emphasizes the importance of “regulatory harmonization and the need for a safe harbor concept that allows for the adoption of acceptable frameworks and standards in

certification standards.” A harmonized regulatory environment would enable more fluid transnational transactions and better data flow within nation states.



“Localized data centers have become significant aggregation points, attracting the attention of both cybercriminals and state-sponsored attacks.”

Ganesh Subramanya

Cyber Warfare and Localized Data Centers

Data aggregation is not merely a compliance issue. It comes down to performance and data processing efficiency. “Data sovereignty requires data to be concentrated in a way that allows it to be dispersed across different jurisdictions. Latency is still important, and data centers are always going to be in proximity, whether jurisdictionally driven or not,” explains Mark Hughes.

However, with the rise of data residency requirements, “localized data centers have become significant aggregation points, attracting the attention of both cybercriminals and state-sponsored attacks,” argues Ganesh Subramanya.

“Anytime you add a new attack surface into an environment with valuable data, there’s likely to be more attacks and more interest in it.”

Brian Roddy

Dr. Avesta Hojjati reflects the same sentiment on the heightened risks for hosting countries. “If you’re a country hosting these data centers, then you are now a target for cyber-physical attacks.” It is ultimately about expanding the attack surface. Having data centers in specific locations can increase the risk of targeted attacks. “Anytime you add a new attack surface into an environment that has valuable data, of course, there’s likely to be more attacks and more interest in it,” explains Brian Roddy.

Duncan Jones brings to the fore the potential of data centers as targets in future conflicts. “Data centers could be the target of future

wars rather than land,” he suggests, pointing to the strategic value of data in modern warfare. War making is no longer a kinetic act. It heavily involves the cyber domain; digital infrastructure and the data that fuels all cyber-enabled operations. “Adversaries are willing to do whatever it takes to obtain valuable data, which means executives need to take necessary measures to safeguard their data,” underscores Jones.

However, cyber threats occupy only one side of the coin. These big data centers need excessive physical protection as well. Physical attacks, like traditional sabotage, will most likely target the power and cooling facilities of these data centers. “The biggest issue with data centers is power and cooling, which are linked,” says Mark Hughes. To ensure data sovereignty, organizations need to do their part well enough. Latency and sovereignty are not absolute, but they should not be the sole determinants of data sovereignty.

In light of these challenges, Agnieszka Bruyere suggests a move toward a distributed data storage model. “I think that having a distributed model avoids exposing the business to cyber-attacks and other material damages such as data center fires, earthquakes, floods, etc.” Alex Meek-Homes shares the same solution. “Choosing another region in another continent gives you an incredible amount of resilience.” The situation in Ukraine, where offsite data storage proved crucial in maintaining governmental operations during the invasion, exemplifies the importance of geographic diversification for data resilience.

Brian Roddy suggests an innovative solution in the form of “data embassies” – secure storage of data in a foreign country while maintaining sovereignty. This concept could balance the need for local data presence with security and data protection concerns. Roddy also predicts that the “data embassy trend will grow over time.”

Whatever the approach might be – centralized or distributed – Ganesh Subramanya stresses the responsibility of cloud service providers in designing and operating these centers with cyber resilience as a core principle. In addition to these design criteria, customers, especially those in critical infrastructure, must understand the security and resilience of the architectures they are subscribing to. As such, Duncan Jones suggests that data centers may need to offer “varying levels of security based on the sensitivity of the data they host, which could become a competitive advantage.”



“Data centers could be the target of future wars rather than land.”

Duncan Jones

What is the Future of Data Transfers?

Geopolitical Dynamics and Data Sovereignty

The landscape of data transfers and processing is rapidly evolving, influenced by a complex interplay of technological advancements, geopolitical dynamics, and regulatory frameworks.

Agnieszka Bruyere's vision underscores the growing influence of geopolitical factors on data transfers and processing. She insightfully states, "Data flows are primarily determined by geopolitical considerations, rather than by the availability of cyber resources." The European Union's stance, particularly in light of events like the Ukrainian conflict, exemplifies a shift towards data-sharing alliances influenced by geopolitical trust and security concerns.

While Alex Meek-Holmes focuses on the influential role of Europe in setting global data privacy standards, Tony Baudot predicts that "In the next few years, we will see an increase in the number of countries adopting strict data sovereignty laws." However, to balance innovation and national security Baudot predicts a future where "sensitive data is processed within sovereign territories, while less sensitive data utilizing global technologies."

AI and Data Management

However, data sovereignty and privacy-respectful data management are going to be challenged by the evolution and pervasiveness of generative AI models and platforms.

Brian Roddy presents a compelling dilemma faced by nations in the context of AI: "Can I keep all my data in-country to keep it sovereign, or am I going to be completely disrupted by my competitive nation because they have better access to AI technology?" Roddy's question captures the struggle for a strategic balance between maintaining data sovereignty and staying competitive in the AI race, emphasizing the need for policies that accommodate both objectives. The European Union's AI Act and other AI-related initiatives in the United States and elsewhere are clear indications of this dilemma.

Adding to Roddy's concerns, Michael Tadault expresses uncertainty about future control over data, primarily due to excess data generated and processed by AI: "The amount of data we're going to generate will be spectacular. But I'm not sure about how much control we'll have over it." He reflects on the growing complexity: "It's difficult for humans to comprehend this anymore. It's already complex. So it's going to be more extreme in the future."

"Data flows are primarily determined by geopolitical considerations, rather than by the availability of cyber resources."

Agnieszka Bruyere

"Can I keep all my data in-country to keep it sovereign, or am I going to be completely disrupted by my competitive nation because they have better access to AI technology?"

Brian Roddy

Furthermore, technology advances have shifted the strategies regarding data retention and protection. While the initial guidance of the Payment Card Industry (PCI) was to keep minimal data, the current AI-driven approach is to retain more data for potential insights. Everybody wants to keep all the data everywhere, which means data owners need to make sure that all that data is protected everywhere. This is a trend that highlights the conflict between privacy-driven data minimization strategies and the emerging trend of data accumulation for AI processing and training.

Paradigm Shift in Data Processing

According to the experts, to address the future challenges in data processing and data transfers, there must be a paradigm shift, leveraging novel approaches and technologies.

For example, Duncan Jones's insights pivot the focus towards a data-centric approach. His emphasis on "international dialogue on data" suggests that such discussions are beneficial for strategic alignment and understanding in data protection. "Executives should engage in these dialogues for strategic insights and alignment, as they will enhance understanding and protection of data." Finally, Jones points out that in a data-centric environment, there will be the need for "continuous evolution in how data protection services are offered." He believes that companies that provide such services will have to innovate to anticipate and adapt to changing demands in data protection. "We should consider safeguarding data at every stage of its lifecycle, even at the quantum or atomic level."

The future of data transfers and processing is poised at a critical juncture, marked by rapid technological advancements, evolving geopolitical considerations, and the need for robust privacy and security frameworks. Business leaders must navigate this complex landscape with a strategic approach that balances data sovereignty, technological innovation, and global data connectivity. Adapting to this changing environment requires a keen understanding of the geopolitical implications, the evolving role of AI, and the need for comprehensive data protection strategies.



"We should consider safeguarding data at every stage of its lifecycle, even at the quantum or atomic level."

Duncan Jones



How Thales Enables Data Sovereignty

In today's rapidly evolving digital landscape, maintaining data sovereignty is more critical than ever. Thales is actively shaping strategies and technologies to bolster data sovereignty for businesses globally.

In today's digital landscape, organizations rely on Thales to protect what matters most - applications, data, identities, and software. Trusted globally, Thales safeguards organizations against cyber threats and secures sensitive information and all paths to it — in the cloud, data centers, and across networks. Thales offers platforms that reduce the risks and complexities of protecting applications, data, identities and software, all aimed at empowering organizations to operate securely in the digital landscape. By leveraging Thales's solutions, businesses can transition to the cloud with confidence, meet compliance requirements, optimize software usage, and deliver exceptional digital experiences to their users worldwide.

Best Practices for Data Sovereignty Compliance

This report would be incomplete without offering best practices for being compliant with data sovereignty requirements. Agnieszka Bruyere emphasizes a comprehensive approach to data security, advocating for “360 degrees all-the-data protection mechanism.” She underscores the need for “strong encryption strategies” and robust “backup disaster recovery strategies resilient to cyber attacks,” highlighting the significance of encryption level, based on data sensitivity and a balanced approach to encryption, especially with external HSM usage. Bruyere also champions “transparency and control over data,” advocating for clear policies that enable customers to manage their data usage and protection.

Chris Hickman’s insights focus on cloud migrations, stressing the importance of “understanding the data you’re moving.” He points out that successful cloud migration involves deep knowledge of the data’s nature and sensitivity. Hickman also advises on the necessity of being aware of data residency and its protection in various jurisdictions, essential for executives in data classification and residency understanding as part of their cloud strategies.

Ganesh Subramanya highlights the importance of retaining control over data in public cloud environments through “robust data management and governance practices.” He advocates for “employing technical measures such as encryption and pseudonymization,” using digital certificates from trustworthy sources and adopting quantum-safe algorithms. Emphasizing secure key management, Ganesh Subramanya sees automation as critical for managing security in cloud services, and advises staying informed about innovations in cloud security and data sovereignty.

Ganesh Subramanya and Duncan Jones suggest a forward-looking perspective on quantum computing, with a recommendation to stay informed about quantum-resistant algorithms. Duncan Jones also emphasizes effective governance and classification to manage data properly.

Mark Hughes discusses Zero Trust Network Access (ZTNA) as essential for data sovereignty, focusing on the foundational role of digital identities in data sovereignty and security. Hughes delves into the complexity of identity governance, highlighting its significance in managing data access. “In the context of identity governance, organizations must consider the identity of employees, service accounts, and bots running routine tasks. This complexity can lead to issues such as attacks, escalated privileges, and phishing.”

Lastly, Michael Tadault points out the indispensability of comprehensive data classification for effective data protection, combining encryption with stringent access control. He emphasizes the ongoing nature of data control through regular audits and compliance checks, underlining that data protection is not a set-and-forget scenario, but an evolving process.

The following table acts as a checklist to help businesses keep track of the actions required to ensure resilient data protection in support of data sovereignty concerns:

Key takeaways

Business Challenges

Data sovereignty presents several challenges that business need to address to turn compliance into an advantage.

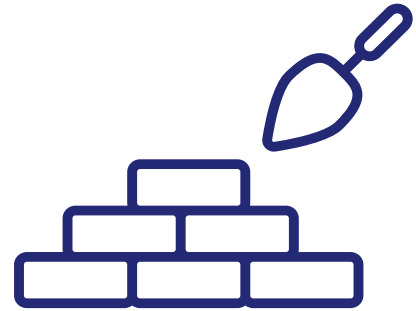


- Extraterritorial Impact vs. Resilience
- Balancing Security, Usability, and Governance
- Data Classification
- SaaS Legal Complexities

Impact on Cloud Strategies

As businesses rely on multiple cloud environments for growth, efficiency, and scalability, they need to consider the impact of operating across borders and jurisdictions.

- Fragmented Legal Environment
- Localization of Operations
- Spacialized, Tailored Cloud Services
- Financial Constraints



Foundations

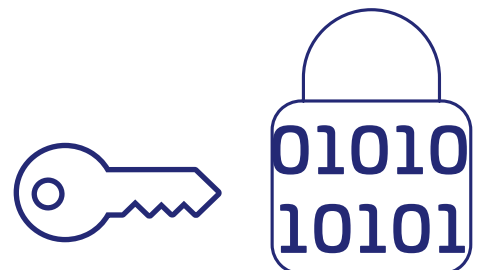
Data sovereignty is based on three foundations.

- 1 Balance Encryption, Compliance, and Resilience
- 2 Key Ownership and Management
- 3 Future-proof Technologies

Key Management vs. Data Sensitivity

Managing encryption keys is essential, but it must align with the growing sensitivity of data and the legal landscape.

- 1 High-Watermark
- 2 Hybrid Model
- 3 Central Repository
- 4 Flexible and Risk-Informed



Impact of Emerging Technology

Emerging technologies bring opportunities, but they also unearth new risks and challenges that business need to consider to ensure safe and compliant innovation.

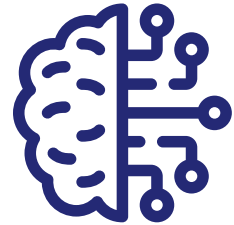


Quantum Battle vs. Post Quantum Cryptography



5G vs. Data Sprawl

Generative AI and Data Explosion



Data Sovereignty and Innovation

Data sovereignty should not be viewed as a barrier to business growth. On the contrary, it can be an enabler for innovation and responsible data governance.

Catalyst for Innovation

Data Responsibility Culture

The Rise of PETs



Strategy and Geopolitics

Data sovereignty efforts should not be examined in isolation. Businesses must consider broader geopolitics and strategic factors and developments.



Internet Balkanization?



The Future of Data Transfers



Data as a Warfare Target

Data Sovereignty Compliance Checklist

Use this checklist to track your progress in ensuring resilient data protection and compliance with data sovereignty requirements. Each item includes a priority level, key actions, and relevant metrics or resources.



Data Protection and Encryption

1 Implement 360-degree data protection mechanism

Priority: High

Actions:

- Conduct a comprehensive data audit
- Implement multi-layered security controls
- Establish continuous monitoring processes

Metric:

Percentage of data covered by protection mechanisms

Resource:

[NIST Cybersecurity Framework](#)

2 Develop strong encryption strategies and pseudonymization

Priority: High

Actions:

- Identify sensitive data requiring encryption
- Implement appropriate encryption methods, including quantum-safe algorithms
- Develop pseudonymization techniques for applicable data

Metric: Percentage of sensitive data encrypted

Resource:

[ENISA Pseudonymisation Techniques and Best Practices](#)

3 Establish effective key management

Priority: High

Actions:

- Implement a robust key management system
- Define key rotation policies
- Ensure secure key storage and backup

Metric:

Frequency of key rotations

Resource:

[NIST SP 800-57 Recommendation for Key Management](#)



Data Governance and Management

4 Implement data classification and governance

Priority: High

Actions:

- Develop a data classification scheme
- Classify all data according to sensitivity and criticality
- Implement access controls based on classification

Metric:

Percentage of data classified

Resource:

[ISO/IEC 27001 Information Security Management](#)

5 Ensure transparency and control over data

Priority: Medium

Actions:

- Implement data lineage tracking
- Provide user-friendly data access and control interfaces
- Regularly audit data access and usage

Metric:

Time to fulfill data subject access requests

Resource:

[GDPR Data Subject Rights](#)

6 Develop robust data management and governance policies

Priority: High

Actions:

- Create comprehensive data governance policies
- Establish a data governance committee
- Implement policy enforcement mechanisms

Metric:

Policy compliance rate

Resource:

[DAMA Data Management Body of Knowledge](#)



Cloud and Infrastructure Security

7 Implement automation in security management

Priority: Medium

Actions:

- Identify security processes suitable for automation
- Implement security orchestration and automated response (SOAR) tools
- Regularly review and update automation workflows

Metric:

Percentage of security processes automated

Resource:

[Gartner SOAR Solutions Guide](#)

8 Understand the nature of data in cloud migration

Priority: High

Actions:

- Conduct pre-migration data assessment
- Develop data-specific migration strategies
- Implement post-migration verification processes

Metric:

Successful data migration rate

Resource:

[Cloud Security Alliance Cloud Controls Matrix](#)

9 Implement Zero Trust Network Access (ZTNA)

Priority: High

Actions:

- Develop a ZTNA strategy
- Implement strong authentication mechanisms
- Establish continuous monitoring and verification processes

Metric:

Number of security incidents prevented by ZTNA

Resource:

[NIST SP 800-207 Zero Trust Architecture](#)

Compliance and Future-Proofing



10 Conduct regular audits and compliance checks

Priority: Medium

Actions:

- Establish an audit schedule
- Conduct internal and external audits
- Implement a system for tracking and resolving audit findings

Metric:

Time to resolve audit findings

Resource:

[ISO 19011 Guidelines for Auditing Management Systems](#)

11 Develop crypto agility and quantum-resistant algorithms awareness

Priority: Medium

Actions:

- Stay informed about post-quantum cryptography developments
- Assess current cryptographic implementations for future risks
- Develop a roadmap for transitioning to quantum-resistant algorithms

Metric:

Percentage of systems ready for post-quantum cryptography

Resource:

[NIST Post-Quantum Cryptography Standardization](#)

12 Maintain data residency awareness in different jurisdictions

Priority: Medium

Actions:

- Create a data residency map
- Stay updated on international data protection regulations
- Implement geo-fencing for data storage and processing where necessary

Metric:

Compliance rate with data residency requirements

Resource:

[IAPP Global Privacy Law Directory](#)



Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com

