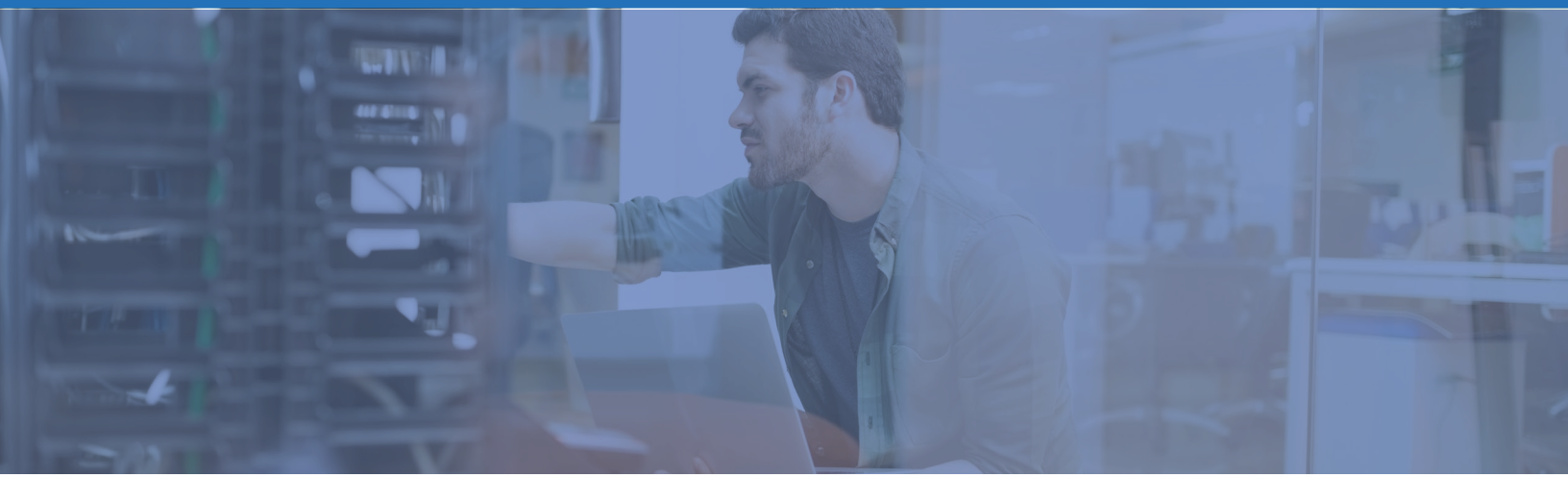
SCALE COMPUTING

Data Sovereignty, Data Residency, and Data Localization: An Introduction

From the Experts at Scale Computing

Technical White Paper

Table of Contents



Introduction

Different countries and regions have varying data protection laws, requirements, and standards, which can dictate how data should be handled, stored, and accessed. These regulations often aim to protect personal information, ensure data security, and prevent unauthorized access or disclosure.

Consequently, it becomes crucial to determine which jurisdiction's data sovereignty applies to your data at any given time. With over 100 countries having data sovereignty laws, navigating these legal constraints can be extremely challenging.

This white paper aims to provide an introduction to data sovereignty, data residency, and data localization. It will explore the diverse laws existing in several key countries and offer helpful guidelines to ensure compliance with data laws.

Let's examine how your data is affected when it resides in various locations, including the United States, Canada, the United Kingdom, the European Union, South Africa, and Japan.

Note: This document, as well as any other materials related to compliance, data sovereignty, or data privacy provided by Scale Computing, does not constitute legal advice. Customers are solely responsible for assessing and meeting their own legal and compliance requirements. It is recommended that customers consult with legal professionals to ensure they understand and fulfill their specific obligations in relation to data sovereignty.

What is...?

Data Sovereignty

Defining data sovereignty can be challenging as there is no universally agreed-upon definition. Different interpretations exist, ranging from individual control over personal data to the ways companies utilize data or even the idea that states should have authority over data created within their borders. However, for the purpose of this guide, data sovereignty will be defined within the broad legal context:

Data sovereignty refers to the understanding that data owners or controllers must be aware of relevant laws to ensure compliance and avoid violating restrictions on data usage and processing. Depending on the location, data owners may need to demonstrate compliance with these laws by accounting for their data.

It is important to note that data sovereignty can extend beyond the borders of the country where the data is physically located. For example, the data of a European Union resident stored in the United States is subject to both EU and US data sovereignty laws. Therefore, a more comprehensive definition of data sovereignty is "the extent to which data is subject to the laws of a country, regardless of its storage location."

Data sovereignty should not be confused with data privacy. Data privacy laws, like the European Union's General Data Protection Regulation (GDPR), focus on responsible data protection for individuals. Data sovereignty determines the applicability of these data privacy laws.

Two related concepts often confused with data sovereignty are data residency and data localization. Data residency refers to the physical location where data is stored, without necessarily addressing the governing laws. Data localization, on the other hand, asserts that data cannot leave a particular jurisdiction. While data localization can be an extreme expression of data sovereignty, it is not synonymous with data sovereignty itself.

Data Residency

Data residency refers to the physical or geographical location where data is stored and processed. It is a concept that focuses on ensuring that data is subject to specific legal and regulatory frameworks based on its physical location. Data residency is particularly relevant in the context of cloud computing and international data transfers.

Data residency is relevant for organizations and individuals as it directly impacts data privacy, security, and compliance with local laws and regulations. Organizations may be required to adhere to data residency requirements due to legal obligations, industry regulations, or contractual agreements. For example, certain countries require that the personal data of their residents be stored and processed within their jurisdiction to maintain data sovereignty and protect individuals' privacy rights. Failure to comply with data residency requirements can lead to legal consequences, reputational damage, and loss of customer trust.

Data residency compliance can be achieved through various means. Organizations may choose to establish their own data centers in specific locations, ensuring that data remains within the boundaries of a particular jurisdiction. Alternatively, they may opt to use cloud service providers that offer data centers located in specific regions or countries to meet data residency requirements.

Data residency considerations also extend to cross-border data transfers. When data is transferred from one jurisdiction to another, organizations must ensure compliance with applicable data protection laws, obtain necessary consents or permissions, and assess the adequacy of data protection measures in the receiving country.

Overall, data residency plays a critical role in data governance, privacy, and compliance strategies. It requires organizations to carefully assess and plan their data storage and processing practices to align with legal and regulatory requirements in different jurisdictions. By understanding and implementing data residency requirements, organizations can effectively protect data, maintain regulatory compliance, and build trust with their customers and stakeholders.

Data Localization

Data localization refers to the practice of storing and processing data within the borders of a specific country or region. It involves imposing restrictions or requirements on organizations to ensure that certain types of data remain within the jurisdiction where it was generated or collected. Data localization is typically driven by regulatory, security, and national interest considerations.

The primary goal of data localization is to exercise greater control over data, protect national security, safeguard privacy, and promote economic interests within a particular jurisdiction. By requiring data to be stored and processed locally, governments aim to ensure that sensitive information remains within their legal and regulatory reach. This can involve imposing restrictions on cross-border data transfers or mandating that data be stored on local servers.

Data localization can be motivated by a variety of factors. National security concerns may drive governments to require critical data, such as defense-related or classified information, to be stored and processed within their borders. Similarly, data related to public health, financial systems, or infrastructure may be subject to localization requirements to ensure regulatory oversight and protect against external threats.

Privacy and data protection also play a role in data localization. Some countries implement localization measures to ensure that personal data of their citizens is subject to their domestic data protection laws. This is often seen as a way to enhance privacy and prevent unauthorized access or misuse of personal information.

However, data localization can have potential drawbacks and challenges. It can disrupt global data flows, hinder international trade, and impose additional costs on businesses. It may limit the ability of organizations to efficiently manage and analyze data on a global scale, impacting innovation and economic growth. Compliance with multiple localization requirements across different jurisdictions can also be complex and burdensome for multinational organizations.

The debate around data localization is ongoing, as different countries and regions have adopted varying approaches. Some countries have embraced data localization as a means to assert sovereignty and protect their interests, while others prioritize the free flow of data and advocate for cross-border data transfers with appropriate safeguards
.

Data Sovereignty, Residency, and Localization Challenges

Complying with data regulatory compliance requirements can be a complex task for organizations, particularly as they grow and operate across multiple countries. Here are some of the challenges associated with adhering to data sovereignty laws:

Rapid changes. These laws are relatively new concepts, and laws surrounding it are evolving rapidly. These changes can sometimes be positive, allowing for legal data transfers between countries. However, they can also introduce additional restrictions and complexities.

Growth. As an organization accumulates more data, understanding which data sovereignty laws apply becomes increasingly complicated. Expanding beyond the original country of origin or serving global clients can lead to a stack of data sovereignty requirements.

Data mobility. New laws may impose restrictions on the movement of data between countries. This can limit the availability of certain cloud services and data storage locations. Data compliance requirements may also dictate specific encryption measures for data in transit and at rest, which may not be feasible with every data transfer method.

Transparency. Demonstrating compliance data laws requires a level of technological transparency, showing how data moves within an organization's IT operations. However, providing such transparency can be challenging, especially for companies with limited resources or complex IT structures that involve shadow IT practices.

The cloud. While the cloud has numerous benefits, its distributed infrastructure can pose data sovereignty challenges. Organizations must be cautious to ensure that their cloud deployments comply with the data laws of different regions. Compliance requirements may also limit their choices and increase costs when selecting cloud services.

Violation risks. Governments enforce data laws with fines, and non-compliance can strain the relationship between an organization and a country, potentially leading to a loss of business. Violations of data sovereignty may even result in prosecution, depending on the severity of the offense.

Increased costs. Achieving data compliance can incur additional operational costs. These may include training on new laws, making changes to the data layer to accommodate regulatory requirements, and implementing necessary security measures.

Navigating these challenges requires organizations to stay informed about evolving laws, adapt their data management practices, invest in appropriate infrastructure, and ensure compliance to avoid penalties, reputational damage, and loss of business opportunities.

Cloud Shared Responsibility Model - Data Sovereignty

Understanding the cloud shared responsibility model is crucial in the context of data sovereignty. This model clarifies the responsibilities of both cloud users and cloud providers in a deployment.

Cloud providers are accountable for maintaining the infrastructure and services offered on a pay-per-use basis. They are responsible for ensuring the availability, reliability, and security of the cloud platform.

Cloud users bear the responsibility for their data and ensuring its safety, protection, and compliance with relevant laws, including data sovereignty regulations. This means that the onus is on the users to understand and adhere to the data sovereignty requirements applicable to their data.

It is important to recognize that in the cloud shared responsibility model, if your data fails to comply with local data sovereignty laws, it is your responsibility as the user, not the cloud provider's. While the cloud provider may offer security measures and compliance frameworks, the ultimate responsibility for data sovereignty compliance lies with the user.

On-Premises Solution

On-premises infrastructure provides a robust solution to address the shared responsibility of data sovereignty in the cloud. By hosting data locally within an organization's own premises, businesses can maintain complete control over their sensitive information, ensuring compliance with data protection regulations and minimizing the risk of unauthorized access or data breaches.

With on-premises infrastructure, organizations can define and enforce their own security policies, implement stringent access controls, and deploy customized encryption mechanisms. This level of control enables businesses to safeguard their data from potential vulnerabilities and maintain sovereignty over their critical information.

Data Regulatory Agencies by Country

Data sovereignty imposes limitations on the handling of your data in various countries.

United States (US)

When it comes to data sovereignty in the United States, it is however essential to consider the various state laws. Operating within the US requires an understanding of these specific regulations as they may differ in terms of data origin, storage, and usage.

Unlike many other countries discussed later in this document, there is no single federal data privacy law in the US. However, there is a strong inclination to resist data localization, which has been addressed in some legislative updates such as those related to NAFTA. NAFTA prohibits data localization for private sector enterprises, putting the onus on organizations to ensure data privacy before it can cross borders. The Federal Trade Commission (FTC) has jurisdiction over some federal-level violations regarding data privacy.

Given the complex landscape of data sovereignty in the US, it is important to stay informed about evolving laws and seek legal guidance to meet the specific requirements applicable to your data operations.

One significant aspect of data sovereignty in the US revolves around the state of California. While California is just one state among the 50 in the country, it possesses the largest gross state product, amounting to $3.2 trillion. If California were an independent nation, its GDP would rank among the top five globally. Additionally, California is home to a significant portion of the US-based tech industry, making data sovereignty regulations within the state particularly relevant.

California Consumer Privacy Act (CCPA) The California Consumer Privacy Act of 2018 (CCPA) stands out as one of the most comprehensive data privacy laws ever implemented in the United States. While often compared to the well-known General Data Protection Regulation (GDPR) of the European Union (which will be discussed in detail later), CCPA differs in its scope, reach, and objectives.

This legislation empowers individuals to have control over how businesses utilize their personal data. The CCPA grants several important rights to Californians, including:

1. The right to request the deletion of their data.
2. The right to opt out or refuse the sale of their data.
3. The right to receive reports on how their personal data is being used.
4. The right to non-discrimination for exercising any of these rights.

As a landmark piece of legislation, the CCPA is expected to inspire the development of similar state-level privacy laws throughout the United States. However, the proliferation of these new laws may pose additional challenges for organizations striving to achieve compliance, particularly when confronted with multiple domestic data privacy statutes within the country.

Virginia Consumer Data Protection Act (VCDPA) Since January 1, 2023, the Virginia Consumer Data Protection Act (VCDPA) has been fully enforced in the Commonwealth of Virginia. This act aims to ensure that Virginia's citizens are adequately protected in the face of the challenges presented by the modern internet era. Data protection and privacy are evolving areas of the law that will continue to grow and pose challenges for businesses and citizens in Virginia.

The VCDPA encompasses various key elements, including expanded consumer privacy rights, a comprehensive definition of personal information, the establishment of sensitive data protection, and data protection requirements for those who manage and control data. It applies to individuals or entities that conduct business in Virginia, produce products or services targeted to Virginia residents, and meet either of the following criteria:

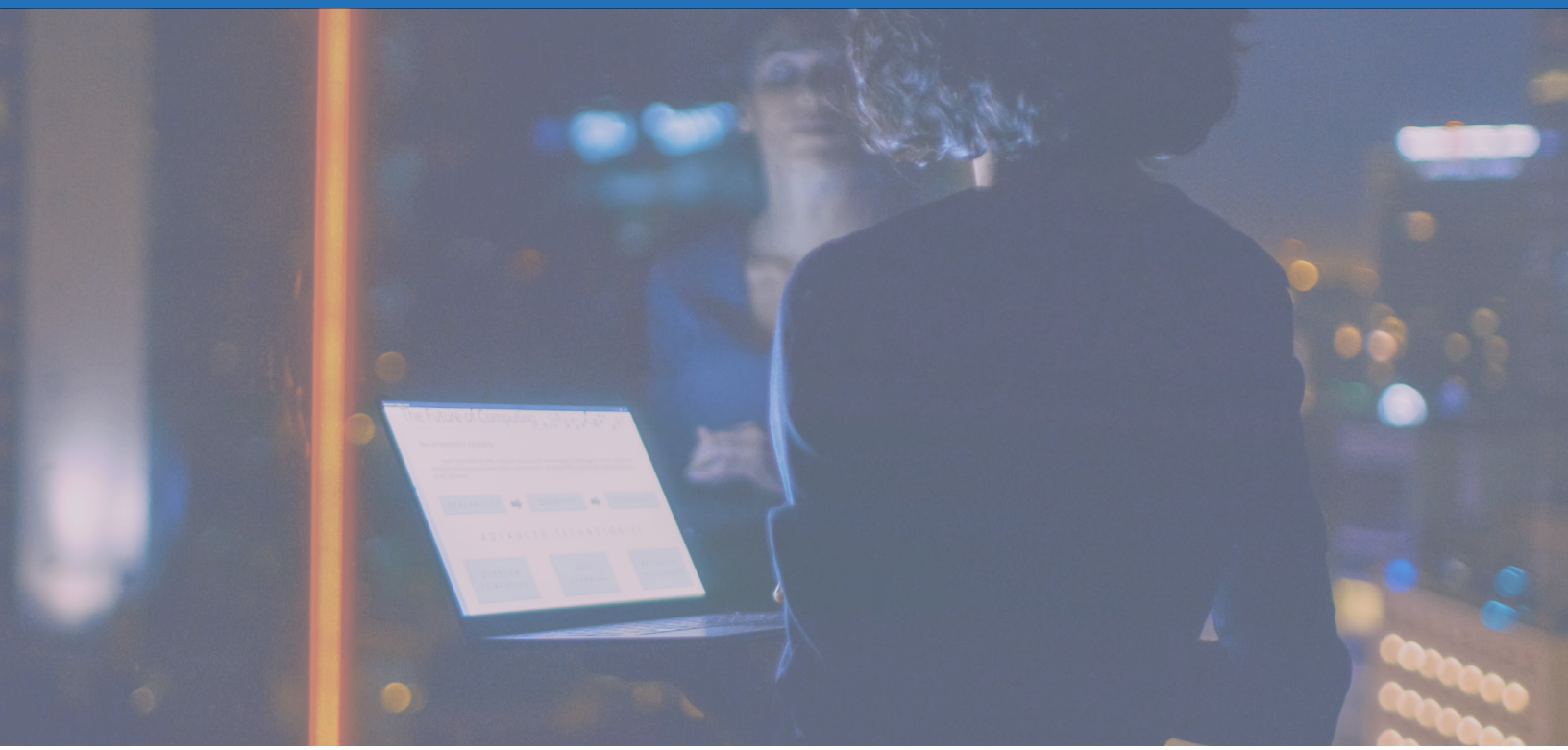
1. Control or process personal data of at least 100,000 consumers during a calendar year.
2. Control or process personal data of at least 25,000 consumers while deriving over 50 percent of gross revenue from the sale of personal data.

Certain entities, such as those subject to HIPAA, not-for-profit organizations, higher education institutions, financial institutions, and data covered by the Gramm-Leach-Bliley Act, are exempt from the VCDPA's requirements.

The VCDPA defines "personal information" broadly as any information linked or reasonably linked to an identified or identifiable natural person. Additionally, it introduces a category called "sensitive data," which includes personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, citizenship or immigration status, genetic or biometric data for identification, personal data of known children, and precise geolocation data.

Businesses subject to the VCDPA must conduct and document a data protection assessment if they process sensitive data, sell personal data, or process personal data for targeted advertising or profiling purposes.

While there is no private right of action provided, the Virginia Attorney General's office is responsible for enforcement, and violations can result in fines of up to $7,500 per violation. It is crucial for organizations to be aware of their obligations under the VCDPA to ensure compliance and avoid penalties.



Canada

Similar to the United States, Canada has data sovereignty laws at both federal and provincial levels.

Personal Information Protection and Electronic Documents Act (PIPEDA) The primary federal legislation governing data privacy and sovereignty in Canada is the Personal Information Protection and Electronic Documents Act (PIPEDA).

Under PIPEDA, businesses that collect data are obligated to safeguard personal and sensitive data, both during storage and transmission. Consent from data subjects is required for the collection and use of their data. Individuals have the right to know how their data is being used and the ability to correct any inaccuracies.

Furthermore, PIPEDA mandates that data can only be used for the purpose for which it was originally collected. If a company intends to utilize the data for any other purpose, it must seek additional consent from the individuals involved to avoid legal non-compliance.

All businesses that operate in Canada and handle personal information that crosses provincial or national borders in the course of commercial activities are subject to PIPEDA, regardless of the province or territory in which they are based (including provinces with substantially similar legislation).

A significant aspect of PIPEDA is the data localization requirement, which stipulates that data can only be transferred outside of Canada if the receiving country provides equivalent data and cybersecurity protections. This restriction can potentially limit businesses' ability to transfer data, particularly to countries like the United States, where there is no federal law specifically safeguarding user data.

Personal Health and Information Protection Act (PHIPA) The Personal Health Information Protection Act (PHIPA) is a comprehensive legislation in Canada that governs the collection, use, and disclosure of personal health information (PHI) by health information custodians (HICs). PHIPA was enacted in 2004 in the province of Ontario and applies to health care providers, such as hospitals, clinics, and doctors, as well as other organizations that handle PHI.

PHIPA is designed to protect individuals' privacy rights and ensure the confidentiality and security of their health information. It sets out a framework for the proper handling of PHI and establishes rules and obligations for HICs to follow. Here are some key aspects of PHIPA:

- Consent and Individual Rights: PHIPA emphasizes the importance of obtaining consent before collecting, using, or disclosing an individual's PHI. It grants individuals the right to access their own health information, request corrections, and control how their information is shared.
- Security and Safeguards: PHIPA requires HICs to implement reasonable security measures to protect PHI against unauthorized access, use, disclosure, and loss. It also mandates the notification of individuals and relevant authorities in the event of a privacy breach.
- Purpose and Limitation: PHI may be collected, used, and disclosed only for legitimate purposes related to the provision of health care or for other authorized purposes specified by law.
- Information Sharing and Disclosure: PHI sharing between health care providers involved in an individual's care is permitted. However, disclosure to third parties, such as insurers or employers, requires consent or must meet specific legal criteria.
- Accountability and Enforcement: The Information and Privacy Commissioner of Ontario was established as the oversight authority responsible for monitoring compliance with the legislation. The Commissioner has the power to investigate complaints, conduct audits, and impose penalties for non-compliance.

European Union (EU)

Data sovereignty in the European Union (EU) is a dynamic and developing area. Efforts have been made within Europe to establish a robust European-based cloud infrastructure that can enhance data sovereignty across EU member states.

Although individual EU member states such as Germany, Italy, France, and others have their own national data protection regulations and provisions, they are closely aligned with and dependent on EU legislation. This section will primarily address the laws that apply to the entire EU, ensuring consistent data protection standards across the region.

General Data Protection Regulation (GDPR) The General Data Protection Regulation (GDPR) is a comprehensive regulation that is binding and directly applicable to all European Union (EU) member states. The GDPR aims to safeguard the data privacy of all individuals residing in the EU and applies to any organization, regardless of profit or non-profit status, that operates within the EU or controls data belonging to EU residents. As a result, the reach of EU's data sovereignty extends globally.

Under the GDPR, data covered by the regulation cannot be transferred outside the EU unless there is a guarantee that the destination country has comparable data protection laws in place. This provision effectively establishes data localization requirements. The GDPR has served as a model for similar legislation in numerous countries worldwide.

The GDPR covers:

- Timely breach reporting: Organizations are required to promptly report any breaches within a 72-hour timeframe.
- Enhanced individual rights: The GDPR grants individuals, referred to as data subjects, several new rights to protect their personal information. These rights include:
  - The right to erasure, also known as the right to be forgotten.
  - The right to request access to all data that companies hold about them.
  - The right to rectify or correct inaccurate data held by companies (referred to as data subject access requests or DSARs).
  - The right to be informed if their data has been compromised in a breach.
- Data minimization: Organizations are obligated to collect only the necessary data that aligns with a specific and legitimate purpose. This provision aims to counteract the practice of excessive and indiscriminate data collection, where businesses treat data itself as a valuable asset.
- Lawful processing: Personal data can only be processed based on one of the six lawful bases for processing, with consent being one of the lawful grounds. Organizations must ensure that they have a valid legal basis for processing individuals' personal information.

United Kingdom (UK)

The UK Data Protection Act 2018 is a comprehensive legislation that governs the processing and protection of personal data in the United Kingdom. It serves as the UK's implementation of the GDPR in the EU.

The Data Protection Act 2018 builds upon the principles and rights outlined in the GDPR and provides additional provisions that are specific to the UK. It covers various aspects of data protection, including the collection, storage, use, and sharing of personal data by organizations and individuals.

One of the key objectives of the Act is to enhance individuals' rights and control over their personal data. It outlines the rights of data subjects, such as the right to access their personal data, the right to rectify inaccuracies, and the right to request erasure of their data under certain circumstances. It also introduces new rights, such as the right to data portability, which allows individuals to obtain and transfer their data from one organization to another.

The Act establishes the Information Commissioner's Office (ICO) as the regulatory authority responsible for enforcing data protection laws in the UK. The ICO has the power to investigate data breaches, issue fines, and provide guidance to organizations on compliance with data protection requirements. It also has the authority to conduct audits and inspections to ensure that organizations are handling personal data in accordance with the law.

The Data Protection Act 2018 places specific obligations on organizations that process personal data. It requires them to implement appropriate security measures to protect personal data from unauthorized access, loss, or destruction. It also introduces stricter rules for obtaining valid consent for data processing and imposes obligations for organizations to conduct Data Protection Impact Assessments (DPIAs) when processing personal data that presents a high risk to individuals' rights and freedoms.

South Africa

At the time of this writing, the South African government was reviving its consultation process for the National Cloud and Data Policy, which had previously released a draft policy document in April 2021. This announcement was made by Mondli Gungubele, the newly appointed Minister for the Department of Communications and Digital Technologies, during the budget vote speech on May 18, 2023.

According to the Minister, the National Cloud and Data Policy will provide guidelines for government departments to effectively utilize cloud services while ensuring data privacy and security in collaboration with relevant providers. The policy aims to enhance the government's capacity to deliver services to its citizens, facilitate evidence-based policy development through data analytics, and strengthen South Africa's data sovereignty and security.

The initial draft version of the National Data and Cloud Policy, released in 2021, aimed to create a favorable environment for the provision of cloud and data services to promote inclusive socio-economic development. It addresses various challenges, including inadequate and unequal digital infrastructure, limited access to cloud and data services for citizens, and fragmented policies and regulatory frameworks that hinder the growth of a data and cloud-driven economy. The document also highlights concerns about foreign multinationals' role, such as the loss of local data ownership and the barriers faced by new entrants, including small and medium enterprises (SMEs).

Japan

Data protection requirements have been in place in Japan since 2003, but significant changes were introduced in 2015 with the enactment of the Act on the Protection of Personal Information (APPI). This Act was amended in 2020 to include stricter provisions for reporting data breaches, which will come into effect in 2022. The APPI is enforced by the Personal Information Protection Commission (PPC), which plays a crucial role in overseeing compliance with the Act.

One of the key aspects regulated by the APPI is the transfer of personal data to parties located outside of Japan. The Act imposes specific requirements and safeguards to ensure that personal data is adequately protected during such transfers. Additionally, organizations are required to maintain records of all data transfers outside of Japan, ensuring transparency and accountability.

The APPI also addresses the use of anonymized data, establishing rules and guidelines for its handling. These provisions aim to balance the utilization of data for various purposes while protecting individuals' privacy rights.

Furthermore, the amended APPI introduces stricter obligations regarding data breaches. Starting in 2022, organizations are required to take specific actions in the event of a data leakage or breach, ensuring prompt and appropriate response measures are in place to mitigate potential harm to individuals and prevent further unauthorized disclosu

By establishing clear guidelines for data transfers, anonymized data usage, and data breach reporting, the APPI aims to safeguard individuals' privacy rights and promote responsible data handling practices across various sectors in Japan. The enforcement efforts of the PPC play a crucial role in ensuring compliance with these provisions and maintaining a high level of data protection in the country.

Data Compliance Questions to Consider for Your Organization

There are some important questions to ask when considering your organization's compliance with data sovereignty, residency, and localization laws:

- What adjustments can be made to your deployment to ensure better compliance with data sovereignty laws?
- Are your teams aligned regarding data sovereignty?
- Will seeking assistance from third-party services simplify compliance?
- Can you track and verify the movement of data throughout your IT infrastructure?
- Where are your backups stored?
- Where are your backup and disaster recovery systems located?
- What measures are in place to protect data during transit?
- Should you consider migrating to on-premises from the cloud?
- What systems are in place to monitor data movement in hybrid cloud setups?
- What are the data sovereignty implications of moving data out of a specific region?
- How will compliance with data laws affect your overall operational costs?
- Who in your organization is responsible for meeting data compliance requirements?
- Can technology be utilized to monitor your data effectively?
- Are you capable of reporting on the data you own?

How Scale Computing Supports Compliance with Data Laws

Scale Computing is a leading provider of hyperconverged infrastructure (HCI) solutions that empower organizations to achieve compliance with data sovereignty, data residency, and data localization. With its innovative technology and features, Scale Computing offers a comprehensive solution that addresses the complexities and challenges associated with data compliance and protection.

Data Sovereignty. Through its distributed architecture, Scale Computing clusters can be deployed across multiple locations, allowing organizations to keep their data within specific regions or jurisdictions. This ensures that data remains under the control of the organization and within the boundaries required by data sovereignty regulations.

Data Residency. Scale Computing provides flexible deployment options that allow organizations to store and process their data locally. By leveraging its hyperconverged infrastructure, organizations can build private clouds or edge computing environments in their desired locations, ensuring that sensitive data stays within the borders of a specific country or region. This capability is particularly important for industries such as government, finance, healthcare, and defense, where strict data residency requirements exist.

Data Localization. With its ability to deploy clusters in various sites, organizations can ensure that their data is stored locally, reducing the risk of cross-border data transfers and potential non-compliance with data localization regulations. This is especially critical for countries with stringent data sovereignty laws that mandate data to be physically stored within their jurisdiction.

Scale Computing Platform is designed with robust security and data protection features to further enhance data sovereignty, data residency, and data localization compliance. The platform incorporates encryption, access controls, and backup and disaster recovery capabilities to safeguard sensitive data and ensure compliance with regulatory requirements. SC//Platform's "set it and forget it" ability makes it radically easier for organizations to run workloads on-premises (and satisfy requirements) than it is in the cloud.

By enabling organizations to retain control over their data, store it locally, and meet data compliance obligations, Scale Computing plays a vital role in helping businesses navigate the complex landscape of data sovereignty, data residency, and data localization. With its scalable and secure infrastructure, organizations can confidently manage their data while adhering to regional and industry-specific regulations

Corporate Headquarters
525 S. Meridian Street - 3E
Indianapolis, IN 46225
P. +1 317-856-9959
scalecomputing.com

EMEA B.V.
Europalaan 28-D
5232BC Den Bosch
The Netherlands
+1 877-722-5359

SCALE COMPUTING