protiviti®
Global Business Consulting

How data sovereignty and data localization impact privacy programs

The concepts of data sovereignty and data localization stem from a desire to keep data within a country's borders for greater control. While the broad strokes of various privacy laws may be consistent across jurisdictions, governments will dictate the collection, storage and interpretation of their citizens' data through constantly evolving privacy regulations.

The legislative bodies that write the privacy regulations not only scrutinize how personal data is used and the safeguards used to secure it but must also consider how other government entities respect privacy when they may have unfettered access to the data.

With more than $3 billion in fines levied as a result of privacy violations, these recent legal actions highlight the willingness of these governments to empower regulators to enforce privacy regulations and concepts.

Data sovereignty defined

Data sovereignty is the concept of a nation asserting control over personal data collected within its borders. Its focus is on the authority and jurisdiction a country has over that data, including aspects related to ownership, security and access rights. Motivations for asserting data sovereignty include concerns about national security, protecting citizens' data rights and regulating cross-border data flows.

Organizations that collect data are required to meet the legal and regulatory requirements of the country in which the personal data originated. Implementing data sovereignty may require considering the following requirements:

- Minimizing data access to authorized individuals
- Developing and implementing policies to protect data
- Ensuring that any data being transmitted follows security protocols, storage and lifecycle policies, including destruction.

Data localization defined

Data localization is the concept that personal data must be stored and processed within a specific geographical location or jurisdiction. The focus is on the physical location, specifying where personal data should be located and processed. Motivations for data localization include national security, supporting local industry and ensuring compliance with local regulations.

Obligations for organizations can include keeping certain types of personal data collected on servers located within a jurisdiction, with express prohibitions against cross-border data transfers, transfers allowed under a narrowly defined set of circumstances and requirements to obtain consent from a data subject before transferring personal data.

Nation-states typically use data-localization obligations to assert sovereignty over their citizens' personal data.

Recognizing the challenges and concerns

Complying with data-sovereignty and data-localization regulations poses challenges for organizations managing personal data in the global economy. Organizations need to balance local data control and regulatory requirements with the practicalities of cross-border data flows. These challenges impact an organization's compliance efforts, data management practices and global operations.

- **Complexity of regulatory landscape**: Different countries have varying regulations, and the global regulatory landscape is rapidly changing. Complying with diverse and evolving regulations can be highly complex and can lead to legal risks and require significant legal expertise. Compliance costs will increase due to investments in time and resources required to navigate aspects of each jurisdiction where an organization operates.
- **Cross-border transfers**: Additional compliance burdens are associated with reviewing and negotiating service-provider agreements to allow appropriate transfers of personal data, verifying service-provider commitments, ensuring that service providers acknowledge and comply with those requirements, and performing transfer impact assessments. These requirements often hinder international data flows, directly impacting collaboration efforts.
- **Consent management**: Permission-based regulations require organizations to obtain consent from individuals to share or disclose personal data. Failure to meet these obligations can lead to reputational damage, litigation and legal liabilities.
- **Operational costs**: Establishing technical infrastructure in multiple local jurisdictions to comply with localization regulations increases operational costs of organizations operating globally. The desire to assert greater control of personal data and promote the local digital economy may lead to organizations exiting a local market. In addition, organizations may have difficulty identifying all systems that store personal data and deploying appropriate controls for those systems.

Looking ahead

Data-governance and data-localization regulations can have a severe impact on an organization's attempts to do business digitally. The rules and regulations can be complex and can change quickly, which requires organizations to be proactive in their governance of data and to regularly audit their data-privacy program to make sure compliance is maintained. With the growing trend toward data localization and adoption of data-transfer regulations, Protiviti can help organizations prepare for and manage these ever-changing developments.

In our experience, we have found the following to be critical building blocks, among other best practices, when developing a forward-facing privacy program and avoiding costly litigation and regulatory fines:

- Understanding global data-privacy regulations and industry practices and how they apply to your specific business operations
- Performing discovery and documentation pertaining to how personal data flows through your organization and to outside third parties
- Determining whether your organization is transferring data across borders and assessing the impact to individuals' rights
- Ensuring that notices and disclosures are updated and aligned with applicable legal requirements

Nevertheless, data-governance and data-localization regulations will continue to evolve, and it is critical for organizations to keep abreast of the changing regulatory landscape and rely on trusted partners to help ensure that regulations are not violated.

For additional information, examples and insights, visit Protiviti's Data Privacy web page. Protiviti is not a law firm and nothing within this paper should be relied on for legal purposes. Clients should always seek legal advice from inside or outside counsel.

Contacts

Sameer Ansari
Managing Director
sameer.ansari@protiviti.com

Arnold Park
Manager
arnold.park@protiviti.com

Joseph Emerson
Director
joseph.emerson@protiviti.com

Nicholas You
Associate Director
nicholas.you@protiviti.com