Data Sovereignty

Jennifer Morales (C)
Contingent Worker

Data Sovereignty & its Significance

What is Data Sovereignty?

Data Sovereignty refers to the laws and policies of a given (sovereign) nation regarding data. While it’s important to understand what data sovereignty is, there actually isn’t one universally agreed-upon definition.

Some use the term to refer to any one person’s individual right to control their own data. Others see it as a term to address how companies use data, rather than the laws which require them to protect it. Still others use the term to describe the notion that states should have the right to maintain control over data created within their borders.

According to a review of data sovereignty laws - Data sovereignty is the concept that information, which has been converted and stored in binary digital form, is subject to the laws of the country in which it is located.

As Data Sovereignty laws and policies have evolved, the definitions have reached across borders, for example, the data of a European Union resident stored in the United States is subject to GDPR requirements.

Therefore, a more complete definition of data sovereignty would be *“the extent to which data is subject to the laws of a country, no matter where it is stored.”*

What is Data Sovereignty related to (but differs from)?

For clarity, it should be noted that data sovereignty is not synonymous with data privacy. Data privacy laws, such as the European Union’s General Data Protection Regulation (GDPR), relate to how companies can responsibly protect the data of individuals. In this sense, your clients’ data sovereignty determines the applicability of such data privacy laws.

Other similar concepts that might be confused with data sovereignty include **data residency**, which relates to the locations where data is kept (not the laws that govern it), and **data localization**, in which states assert that data cannot leave their boundaries.

Data Localization Laws are driving the location of data, data centers and cloud services for businesses concerned with compliance beyond a single country’s borders.

Sovereignty can also include related issues of Data Location (where governments say data may be located), Data Residency (where companies place the data) and Data Privacy (who has knowledge of the content).

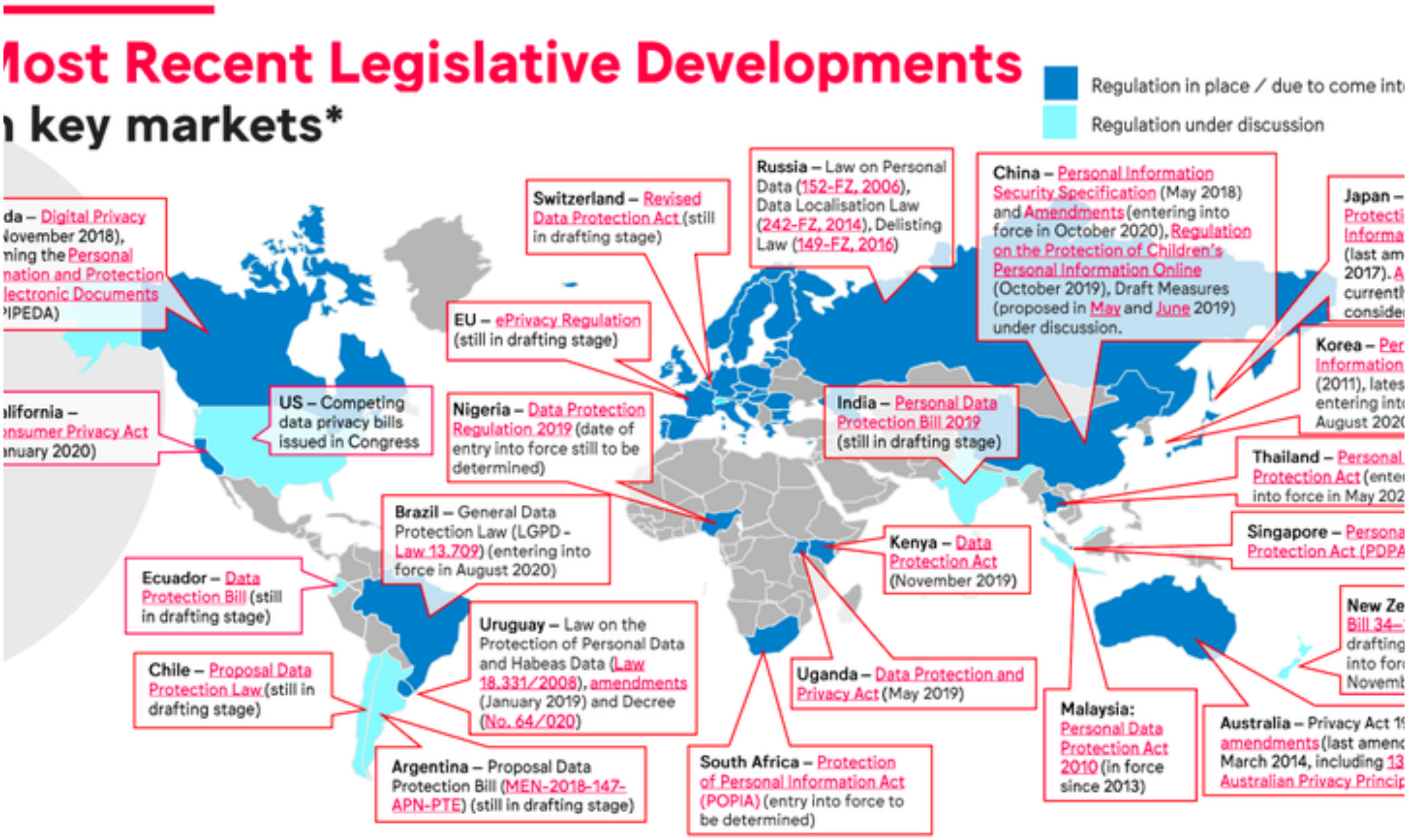
Data Sovereignty – How It Works

Data Sovereignty covers laws about where the data is allowed to be and to whom it relates as well of what type of data is governed (e.g. personal data, financial data, tax data, etc.). This can be based on to whom the data is related (e.g. citizens of the EU) and the location – i.e. where the data is allowed to be located. Examples of location include the EU country of origin, specific EU member states, or the US with master copies kept in the EU. Fundamentally, control in this context is about access to the data, be it in use, in motion or at rest. The definitions vary by jurisdiction. Two topics which have driven the need for the concept include:

1. cross-border transmission of data since it is moving from one jurisdiction with applicable laws to another jurisdiction with its own laws
2. determining legal nexus and governance imposed by nations and indigenous groups as they continue to clarify legal rights for each group

This is further complicated by the fact that controls can be levied below the national level such as with the California Consumer Privacy Act of 2018 (CCPA); and across groups of nations such as the EU's GDPR.

For Vertex, this may sound familiar given our experience with indirect tax law which has shown us the variability and associated complexity of interpretation across jurisdictions and the importance of quick and transparent compliance.


/lost Recent Legislative Developments
ı key markets*
Regulation in place / due to come int
Regulation under discussion

da – Digital Privacy
lovember 2018),
ning the Personal
nation and Protection
lectronic Documents
PIPEDA)

alifornia –
ɔnsumer Privacy Act
ɑnuary 2020)

US – Competing data privacy bills issued in Congress

Switzerland – Revised Data Protection Act (still in drafting stage)

EU – ePrivacy Regulation (still in drafting stage)

Russia – Law on Personal Data (152-FZ, 2006), Data Localisation Law (242-FZ, 2014), Delisting Law (149-FZ, 2016)

China – Personal Information Security Specification (May 2018) and Amendments (entering into force in October 2020), Regulation on the Protection of Children's Personal Information Online (October 2019), Draft Measures (proposed in May and June 2019) under discussion.

Japan –
Protecti
Informa
(last am
2017). A
currentl
conside

Korea – Per
Information
(2011), lates
entering int
August 202(

Nigeria – Data Protection Regulation 2019 (date of entry into force still to be determined)

India – Personal Data Protection Bill 2019 (still in drafting stage)

Thailand – Personal
Protection Act (ente
into force in May 202

Brazil – General Data Protection Law (LGPD - Law 13.709) (entering into force in August 2020)

Kenya – Data Protection Act (November 2019)

Singapore – Persona
Protection Act (PDPA

Ecuador – Data Protection Bill (still in drafting stage)

Uruguay – Law on the Protection of Personal Data and Habeas Data (Law 18.331/2008), amendments (January 2019) and Decree (No. 64/020)

New Ze
Bill 34–
drafting
into for
Novemb

Chile – Proposal Data Protection Law (still in drafting stage)

Uganda – Data Protection and Privacy Act (May 2019)

Malaysia: Personal Data Protection Act 2010 (in force since 2013)

Australia – Privacy Act 19
amendments (last amen
March 2014, including 13
Australian Privacy Princip

Argentina – Proposal Data Protection Bill (MEN-2018-147-APN-PTE) (still in drafting stage)

South Africa – Protection of Personal Information Act (POPIA) (entry into force to be determined)

Data Residency

Data residency is a decision by a business to store their data in a specific geographical location. Businesses may choose a location for the data based on regulatory, performance, or tax considerations.

For example, a company can move data to a certain country to benefit from favorable privacy regulations in that country, or attempt to carry out a specific amount of business in a country to meet its tax benefit requirements. To accomplish this, the organization could make a data residency policy noting that all data should be processed and stored within that country's borders.

Data Localization

A subset of Data Sovereignty is known as Data Localization. People often use the terms data sovereignty and data localization interchangeably. However, data localization is a governmental policy or law that specifies where governments can locate data. An example is the EU’s EDPR, it states that European countries should host all personal information collected on European citizens within the EU within the EER, EU, or several other specified countries.

Localization is a version of data residency predicated on legal obligations. Data localization requires that data created within certain borders stay within them.

In many cases, data localization laws simply require that a copy of such data be held within the country’s borders, usually to guarantee that the relevant government can audit data on its own citizens (provided there is due cause) without having to contend with another government’s privacy laws. India’s draft Personal Data Protection Bill is an example of exactly this. There are countries where the law is so strict as to prevent it crossing the border at all. For instance, Russia’s On Personal Data Law (OPD-Law) requires the storage, update and retrieval of data on its citizens to be limited to data center resources within the Russian Federation.

Data Sovereignty Impacting Businesses

Any company seeking international growth will sooner or later face the question of whether localizing software products is required or not. There is no simple answer to this question, as it all depends on a multitude of aspects related to your business and specific needs. Companies dealing with complaint data may need to create and maintain multiple data centers and complex infrastructures in different jurisdictions, which adds extra cost to operational spending. Furthermore, companies relying upon such services may find they avoid certain markets altogether due to the increased cost of doing business there. This then further affects the attractiveness of different regions when it comes to capital investment and talent retention, with data localization restrictions acting as digital walls between countries.

Examples of Data Sovereignty

Data Sovereignty for select industries : only data related to certain industries cannot leave the country borders (usually such industries are Financial Services, Healthcare, Telecommunications and Government/Defense).

Example: In 2018 the Reserve Bank of India declared that all payment system providers should store payment data in the country, with similar measures planned for E-commerce, Social Media, Telecom and Healthcare. The UAE and Australia have similar measures for Healthcare data while Turkey introduced data localization for Financial services.

Data sovereignty is a governmental policy or law noting data is subject to the data and privacy laws of a specific geographical location : In example, Australia's Privacy Principles (APP). Personal data kept in Australia must meet the 13 standards specified by the APP, including how data is used and collected and a person's rights to access their data.

Data Replication: in this model copy of all compliant data needs to be stored locally and then can cross the country borders.

Example: The revised Indian Personal Data Protection Bill and EU's GDPR require tech firms to have consumers' consent before collecting and processing their data. The data mirroring requirement of this law requires that a copy of data on Indian citizens be stored in India. Similarly, the new Cybersecurity law of 2019 in Vietnam requires online service providers to store citizens' personal data inside the country.

Controlled localization: Less extreme laws that focus on data privacy.

Example: The most obvious case is the EU's GDPR, which allows data transfers to other countries under certain conditions. Data can be transferred to countries that have the same level of data protection as in the EU. Similar laws have been passed in Brazil (General Data Protection Law of 2018), Colombia and Peru.

Summary

Key takeaways:

- Data Sovereignty = Applicability of laws regarding data (who controls it)
- Data Residency = Where the data is
- Data Localization = Where the data is allowed (and not allowed) to be

As laws and policies evolve, big impacts are felt since decisions like where to store and process data are moving beyond being business decisions and moving rapidly into compliance decisions. At a minimum, since Vertex is expanding globally and handling data from more and more nations and customer, we will need to ensure we stay ahead of compliance risks to ourselves and our customers.

On a potential positive note, with arbitrary laws, there may be opportunity to assist customer determining compliance which may take the form of codifying laws into computer logic and data content. This could be an adjacent area for Vertex to explore business opportunities.

Source articles for this page:

- AWS Infrastructure Solutions BrandVoice: 3 Steps To Meeting Your Data Residency Requirements
- Data Sovereignty in the Cloud: Key Considerations
- SAGE Journals: Your gateway to world-class journal research
- Compliance and the Cloud: Data Sovereignty Explained for MSPs - ChannelE2E: Technology News for MSPs & Channel Partners
- 404 Not Found - data-residency index
- California Consumer Privacy Act of 2018
- https://cdn.incountry.com/wp-content/uploads/2020/08/InCountry-Global-Laws.png
- SaaS Adoption and the Data Residency Dilemma - InCountry
- Data Sovereignty vs Data Residency vs Data Localization
- GDPR Data ProtectionData Sovereignty in the Cloud: Key Considerations
- Data localization checklist for global companies
- Personal Data Protection Bill, 2019
- What is GDPR, the EU’s new data protection law? - GDPR.eu
- Data Sovereignty in the Cloud: Key Considerations