Acronis

WHITEPAPER

Data sovereignty around the world

Exploring regulations in Canada, U.S., U.K., E.U., Brazil and Japan

Anyone who has ever traveled internationally knows that laws are different all over the world. Even boarding a plane to get from one country to another comes with a whole host of restrictions: a passport, a visa, sometimes certain immunizations – and that's before all the restrictions COVID-19 has brought with it. The same is true when it comes to data. The data you own is regulated by specific laws in each country, and moving it from one country to another makes it subject to completely different laws. As a consequence, data sovereignty has been conceived to govern adherence to local regulations around the collecting, storing and processing of this data.

This white paper will introduce the basics of data sovereignty, take a look at some of the different laws that exist in several key countries, and give you a few helpful guidelines on what you can do to stay on top of data sovereignty laws.

Data sovereignty: an introduction

Imagine that the data that you own is just like you. In the same way that you are subject to the laws that exist where you live, different countries have specific laws that determine how data residing in that country can be treated and stored, as well as what needs to be done to protect it.

But just like you, data can move around, especially in the age of the cloud, in which services and infrastructure can exist anywhere in the world. This makes it especially important to determine whose data sovereignty you fall under at any given point in time. There are more than 100 countries with data sovereignty laws, making these legalistic constraints extremely difficult to navigate.

Let's look at how your data is affected in each place it resides, including the United States, Canada, the United Kingdom, the European Union, Japan and Brazil .

What is data sovereignty?

While it's important to understand what data sovereignty is, there isn't one generally 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.

However, for the purposes of this guide, data sovereignty will be defined by how it is understood in the broadest legal context:

Data owners or controllers need to make sure that they are aware of these laws in order to avoid violating restrictions on how that data can be used or processed. They may also, depending on the location, need to be able to account for their data in order to show compliance with such laws.

It should also be noted that in some cases, the reach of data sovereignty goes beyond the borders of the country where the data is located; for example, the data of a European Union resident stored in the United States.

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."

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 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. While the latter might be the most extreme expression of data sovereignty, it isn't in and of itself a description of data sovereignty.

However, data localization laws have doubled in the last ten years, clearly demonstrating how this major concern for organizations is only growing.

What data sovereignty is not:

Data privacy: This refers to making sure that sensitive personal data is protected to a higher degree.

Data residency: This means wherever your data resides. It can be subject to multiple claims of data sovereignty.

Data localization: This is about keeping data within a certain region or boundary. For many governments and regulators, this is an important goal.

> "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."
>
> **Hippelainen, L., Oliver, I. and Lal, S. (2017) in "Towards dependably detecting geolocation of cloud servers."**

The challenges of data sovereignty

There are multiple factors that can make compliance with data sovereignty requirements complicated for organizations to meet. Mostly, this is a problem that comes along with success: the bigger you are, the more likely it is your company will have data falling under multiple data sovereignty restrictions.

Some of the challenges that come with being subject to the data sovereignty requirements of one or more countries include:

- **Rapid changes**

  Since data sovereignty is a fairly new concept, the laws that countries enact to establish their data sovereignty are changing at a rapid pace. Occasionally, these changes can be positive, such as when new legislation allows legal data transfers between countries. However, this is not always the case.

- **Growth**

  The more data you have, the more complicated it can become to understand which data sovereignty laws apply to it. As mentioned previously, this is one of the main drawbacks of successful growth. Organizations that grow beyond their original country of origin, or that take on clients from around the world, will quickly find their data sovereignty requirements stacking up.

- **Data mobility**

  New laws can mean new restrictions on how data can be moved between countries. This can limit the availability of certain cloud services and locations for your data. Data sovereignty may also extend to how data can be moved between repositories, requiring certain levels of encryption for data in transit as well as at rest. However, not every data transfer method enables an optimum level of cyber protection.

- **Transparency**

  Being able to show how your data moves within your IT operations is critical to demonstrating compliance with data sovereignty laws; but that level of technological transparency can be difficult to provide. Some companies simply don't have the staff or tools required to describe how their data collection and data use works. Others may have such complex IT operations that individual team members using shadow IT can potentially violate government regulations, without even knowing it.

- **The cloud**

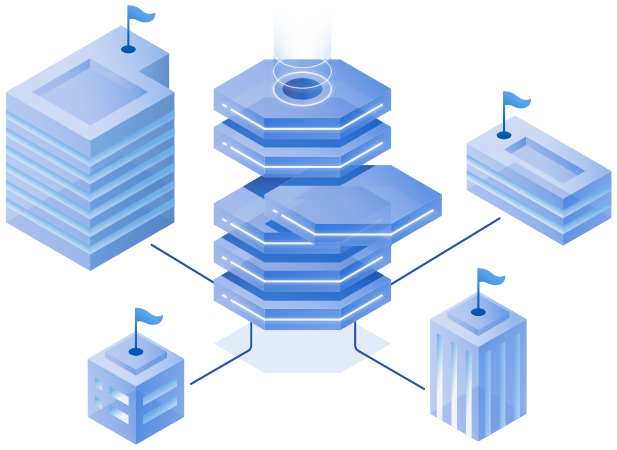
  While its benefits have been innumerable for IT deployments, the cloud itself poses data sovereignty issues due to the dispersed nature of its infrastructure. If organizations aren't careful, their cloud deployments could extend into different regions with different data sovereignty laws. On the other hand, complying with certain data sovereignty strictures may limit their choices when it comes to the cloud services they make available.

- **Violation risks**

  Governments enforce their data sovereignty laws with fines. Not only that, but running afoul of a country's data sovereignty can also cause lasting damage to the relationship between an organization and that country, which may consequently lead to a loss of business. And of course, certain violations of data sovereignty could potentially result in prosecution, depending on the alleged offence.

- **Increased costs**

  Your organization could face increased operational costs due to data sovereignty, from training on additional laws to the data layer changes required to accommodate new rules and regulations.



The cloud's shared responsibility model

Another key concept to be aware of is the cloud's shared responsibility model. In simplest terms, this is a basic delineation between cloud users and cloud providers about which parties are responsible for elements of a deployment.

Cloud providers are responsible for maintaining pay-per-use services and infrastructure. Users are responsible for data and ensuring that it stays safe, protected, and complies with the law. That is where accountability to data sovereignty comes in.

As far as the shared responsibility model is concerned, if your data does not comply with local data sovereignty laws, it's your problem, not your cloud provider's.

Data sovereignty by country

Data sovereignty places constraints upon your data in different countries.

NOTE This document and any other related documentation on compliance, data sovereignty, or data privacy produced by Acronis does not offer legal advice. Customers are solely responsible for evaluating and fulfilling their own legal and compliance obligations.

The United States

When dealing with data sovereignty in the United States, you not only have to be aware of the pertinent laws at the federal level (of which there are many), but also individual state laws. Operating within the U.S. means that you may need to treat your data differently based on where the data comes from, where it's stored and what you do with it.

Some of the most important data sovereignty laws apply to the state of California. This may seem insignificant, considering that California is just one state out of 50, but this state boasts the largest gross state product in the U.S. – $3.2 trillion. If California was a country, that would make its GDP among the top five in the world. And when considering that a majority of the U.S.-based tech industry is located in California, expressions of data sovereignty there are especially relevant.

However, surprisingly, unlike with many of the other countries covered below, there is no single data privacy law for the U.S. at the federal level. There is also a strong imperative to resist data localization, which in some cases has been legislated – as occurred in the recent updates to NAFTA. The Federal Trade Commission (FTC) regulates some violations federally.

California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act of 2018, or CCPA, is probably the most ambitious data privacy legislation ever enacted in the U.S. While this law is frequently compared to the European Union's well-known GDPR, which is covered in depth below, CCPA differs in scope, reach and its ultimate goals.

This legislation allows individuals to have a say over how the personal data that businesses collect about them can be used. The act grants Californians several key rights:

- The right to request their data be deleted
- The right to say no or opt out of the sale of their data
- The right to request reports on how their personal data is being used
- The right to not be punished for invoking any of these rights

As a landmark piece of legislation, CCPA is expected to drive similar state laws in the U.S. However, those new laws may make an organization's compliance even more difficult when there are multiple domestic data privacy statutes to juggle within the country.

Canada

Canada's data sovereignty laws are similar to those of the United States in that Canada also has provincial laws in addition to laws at the federal level.

The Personal Information Protection and Electronic Documents Act (PIPEDA)

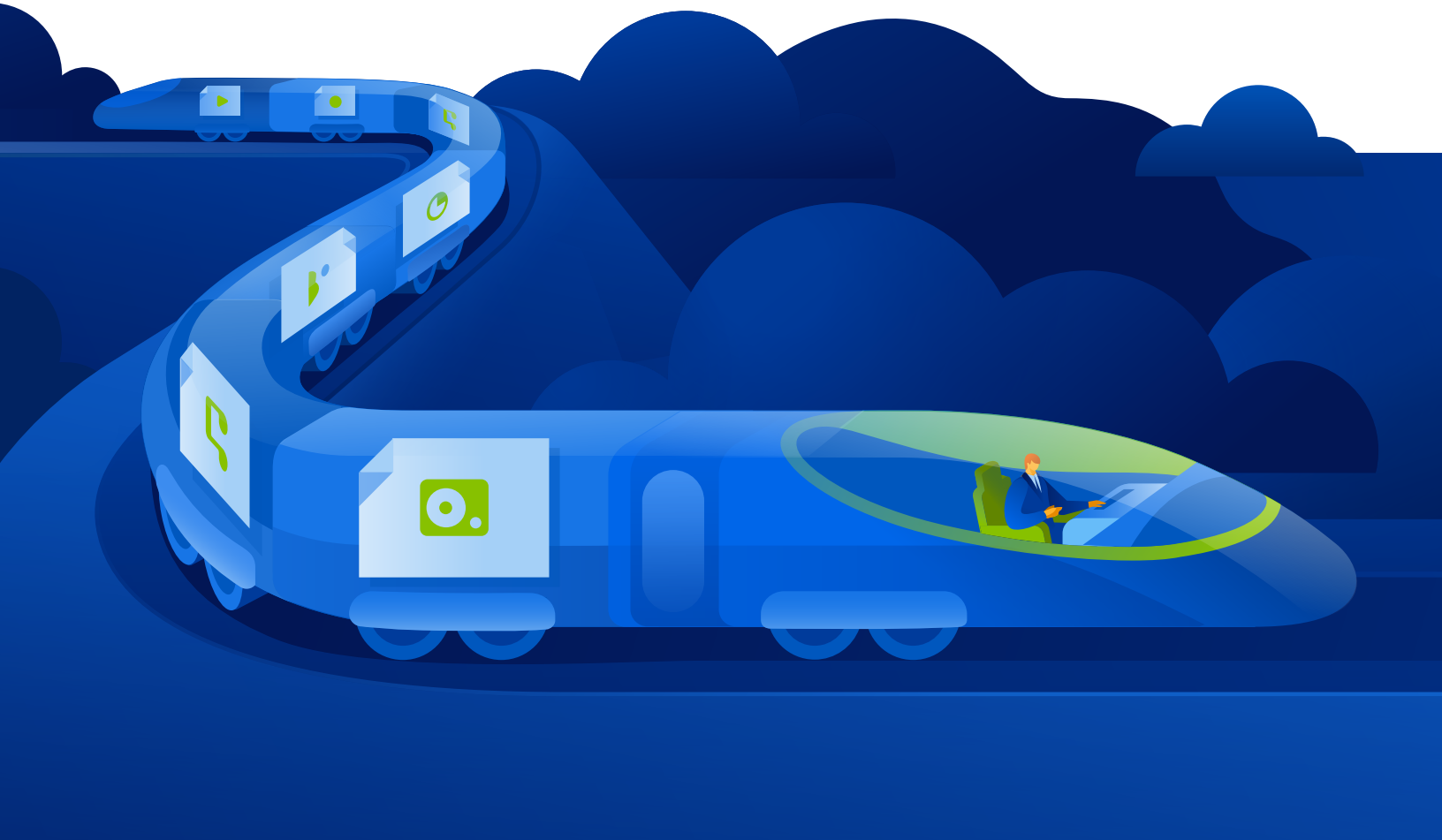
Canada has a federal data privacy law that extends its data sovereignty through a set of strong data localization rules: the Personal Information Protection and Electronic Documents Act, or PIPEDA.

NOTE At the time of this writing, there are provincial initiatives and suggested updates to PIPEDA.

This law states that businesses that collect data must protect personal and sensitive data – both while at rest and in transit. Businesses must obtain their data subjects' consent in order to collect and use this data. Individuals have two rights here: the right to find out how that data is being used and the right to correct it if necessary.

The law also stipulates that data can only be used for the purpose it was initially collected. If a company intends to use the data for any other purpose, it must obtain further consent from the individual subjects of the data – or risk legal noncompliance.

The data localization aspect of PIPEDA requires that data can only be transferred outside of Canada's borders if the receiving country has equivalent data and cyber protections in place. This can limit businesses' ability to send data; for example, to the United States, where there is no such federal law protecting user data.



The European Union

Data sovereignty in the European Union is an evolving field. There have been calls in Europe to create a stronger European-based cloud infrastructure that can help better ensure data sovereignty within the E.U.'s member states.

While Germany, Italy, France and the rest of the E.U. member states have national data protection regulations and provisions in various legislations, they are heavily dependent on and in line with the E.U legislation. This section will focus primarily on the laws that are in place to cover the entirety of the E.U.

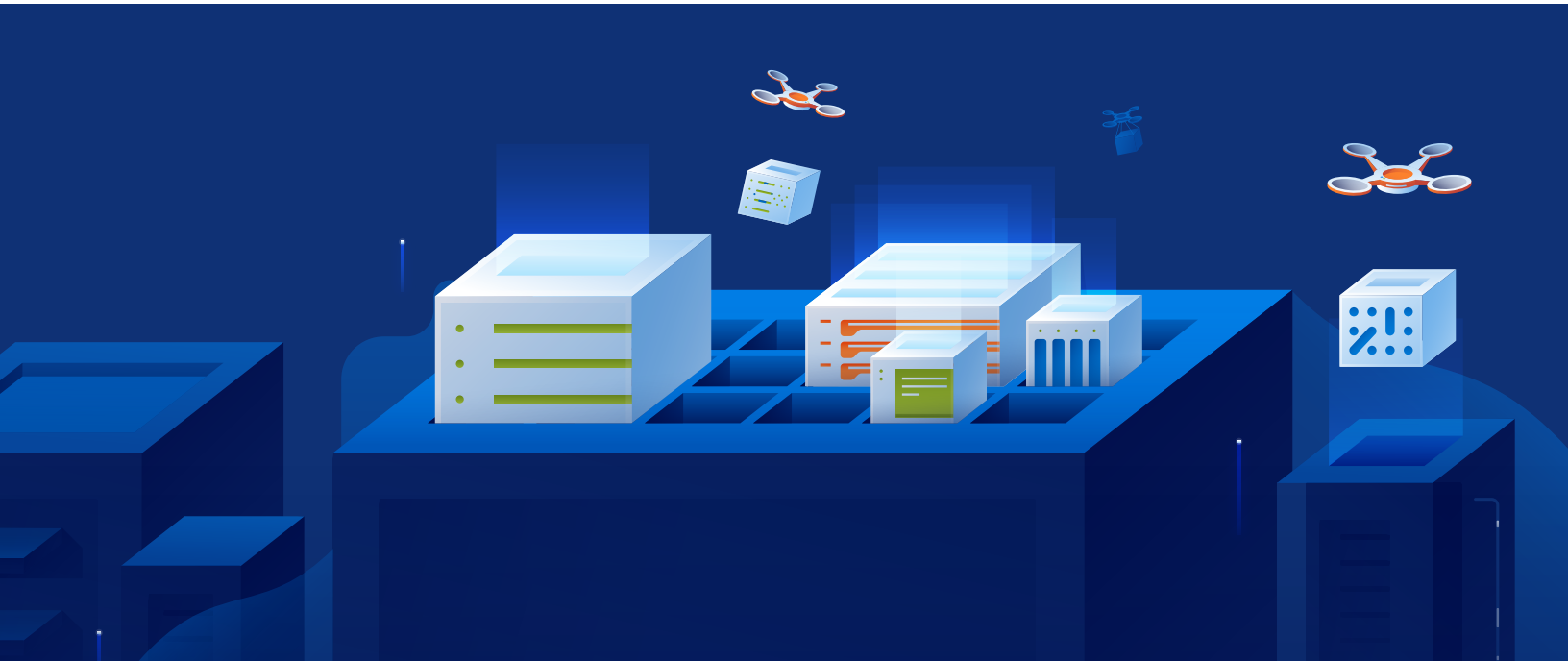
The General Data Protection Regulation (GDPR)

This law might be the most significant expression of data sovereignty in the cloud era. The GDPR is obligatory in its entirety and is directly applicable for all member states. This regulation protects the data privacy of all E.U. residents and applies to any organization – for profit or non-profit – operating in the E.U., or that controls data that belongs to E.U. residents. This effectively extends the E.U.'s data sovereignty to anywhere in the world.

Data applicable to the GDPR is not allowed to be transferred out of the E.U. unless there is an assurance that the country it is being transferred to has a similar data protection law in place. By restricting data transfer outside of the E.U., the GDPR also qualifies as a data localization law. This law has since inspired similar legislation in countries all over the globe.

The GDPR covers:

- **Reporting breaches**: Organizations have a short 72-hour window to notify authorities about any breach likely to result in a risk to the rights and freedoms of natural persons involved.
- **New rights:** GDPR protects individuals (referred to as data subjects in the legislation) by granting them new rights. These rights include:
  - The right to be forgotten
  - The right to make requests for all the data that companies possess about them
  - The right to correct data in a companies' possession (also known as data subject access requests, or DSARs)
  - The right to know if their data has been exposed in a breach
- **Keep data to a minimum:** Organizations can only collect data if it is used with a clear purpose. This addresses predatory data collection, a practice that has been rampant among businesses – which tend to treat data itself as a form of wealth.
- **Lawful processing:** Personal data can be processed only on one of the six lawful bases for processing, consent being one of them.



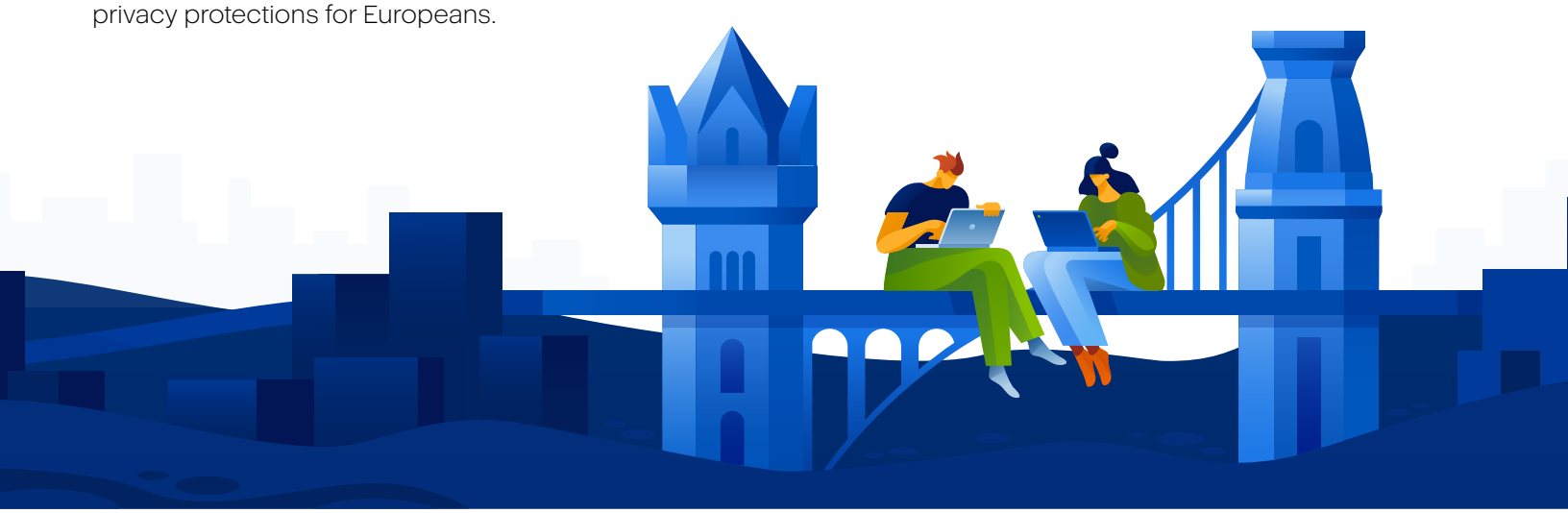
E.U.-U.S. data sharing laws

The GDPR has reset a lot of the data sharing laws that previously made it possible for data to exit E.U. data sovereignty and enter the sovereignty of other countries. This is particularly difficult in the case of the United States.

There's a long history of partnership between the E.U. and the U.S., which extends to how data has been shared between the two countries. However, as we'll read below, the laws that regulate how this is possible have seen a lot of turmoil recently, leaving organizations that have operations on both sides of the Atlantic with difficult problems to solve.

Previously, the International Safe Harbor Privacy Principles were the cornerstone of E.U.-U.S. data sharing and data protection. These were based on seven data sharing principles: notice, choice, onward transfer, security, data integrity, address and enforcement. But by a court ruling in 2015, the Safe Harbor Privacy Principles were invalidated.

International Safe Harbor was followed shortly afterward by a framework called the E.U.-U.S. Privacy Shield. In 2020, this law was also struck down by European courts – after it was ruled that it did not provide sufficient privacy protections for Europeans.



The United Kingdom

Data sovereignty can change quickly, as has been the case in the United Kingdom. Until recently, the U.K. and its residents were protected under the data sovereignty of the EU. But with the passage of Brexit, that's no longer the case.

United Kingdom General Data Protection Regulation (UK GDPR)

The GDPR, as codified for the E.U., no longer protects the U.K. following the U.K.'s withdrawal from the E.U. However, the law is still in effect for the U.K., though in a purely domestic form. The U.K. GDPR is identical to the E.U.'s GDPR in all respects, except that it only protects the data privacy of U.K. and not E.U. residents.

For the U.K.'s part, there is no restriction on transferring data to the E.U., but the same does not go for E.U. data. In June 2021, the European Commission issued a decision that the U.K. under the GDPR regime provides an adequate level of data protection, thus allowing the data flows from the E.U. to the U.K. Yet, this decision is subject to scrutiny. In case of further diversion on a national level from the GDPR principles, the decision can be revoked.

Brazil

Brazil has the largest economy in Latin America and is a member of the BRICS group of emerging global economies (named for its members: Brazil, Russia, India, China and South Africa). With this growth comes an increasing focus on adopting the cloud and cloud-based services. This increasing reliance on cloud-based IT is also being mirrored by the enactment of new data privacy protections that are establishing Brazil's data sovereignty.

Lei Geral de Proteção de Dados Pessoais (LGPD)

The Lei Geral de Proteção de Dados Pessoais (LGPD) – or, the General Personal Data Protection Law – is Brazil's data privacy protection regulation. If the name seems similar to Europe's GDPR, there's a good reason for it: Brazil aimed to create an equally thorough law for protecting private data in their country. However, as we'll see below, there are significant differences in Brazil's legislation which should be considered.

The LGDP was enacted in order to unify the large number of existing state laws that sought to protect private data, but were frequently in conflict with one another. Some elements of the law include:

- **Data privacy:** The LGPD essentially protects the data privacy of all residents of Brazil, no matter where their data is stored.
- **DSAR reports:** The LGPD allows subjects to request full reports on their data, which must be provided within 15 days.
- **Mandatory DPO:** The LGPD mandates the role of a dedicated staff member to maintain an organization's privacy controls.
- **Data transfers:** Data transfers between the E.U. and Brazil are permitted.
- **Oversight:** The National Data Protection Authority (ANPD) was implemented to oversee organizational data stores in order to avoid data loss and breaches, as well as to monitor general compliance with the LGPD.

The LGPD was passed in 2018, but did not come into effect until August, 2021. Both the relative freshness of the law and the delays in its implementation are good indications of why your organization needs to be ready for anything when it comes to data sovereignty.

Japan

The story of Japan's data sovereignty is a cautionary tale – both for other countries and for organizations doing business in Japan. In the past, the Japanese government was reluctant to interfere with businesses – particularly when it concerned data protection. However, a string of incidents in which data breaches exposed the data of millions, prompted a review and update of Japan's primary data protection law, the Act on the Protection of Personal Information.

The Act on the Protection of Personal Information (APPI)

Data protection requirements in Japan have been present since 2003, but were substantially extended in 2015 with the APPI. The Act was amended further in 2020 with stricter provisions for reporting data breaches. Those provisions will take effect in 2022.

The APPI is enforced by the Personal Information Protection Commission (PPC). Some of its key provisions include stipulations on:

- Transferring data to parties outside of Japan
- Recording all such transactions of data outside of Japan
- Rules on how anonymized data can be used
- Effective in 2022, specific actions that need to take place in the event of a data leakage or breach

How you can approach data sovereignty

Researching data sovereignty isn't valuable just for academic purposes. Data sovereignty laws will affect every level of your deployment, from where data is stored, to how it is shared in the development pipeline, to the boardroom office.

In some ways, organizations that are about to make a digital transformation have an advantage here, as they can design their cloud deployments to better align with data sovereignty goals. For deployments that are already in the cloud or straddling the cloud and data centers with hybrid deployments, it may require more effort to make sure all these components can comply with regulations.

Organizations, and especially government and private-sector businesses, tend to operate with strict levels of secrecy. However, this can run contrary to the goals of data sovereignty. Some laws that govern data, such as the GDPR, require users to authenticate how data is used and where it is located. Thus, transparency and "privacy by design and default" should be built into IT operations in order to meet such requirements.

One key to maintaining some degree of flexibility regarding how you approach data sovereignty is to avoid getting locked into any single platform. Where you keep your data will have a big impact on controlling your operational costs and in getting data to most of your users. However, the ease in accomplishing this will depend on where your data is located.

While knowing where you want to keep your data is the first step, you also need to understand how local laws will hold you responsible for keeping that data within a country's borders. Making sure your organization is aligned with relevant data sovereignty laws will require constant attention and care. Data governance tools that can monitor and report on your data to help you understand your legal responsibilities and to convey that information to relevant authorities may help here.

Data sovereignty questions to ask

Here are some important questions to ask when considering your organization's compliance with data sovereignty laws:

- What can you change about your deployment to ensure better compliance with data sovereignty laws?
- Are your teams aligned when it comes to data sovereignty?
- Will turning to assistance from third-party services make things easier?
- Can you verify how data moves throughout your IT deployment?
- Where are your backups located?
- What kind of in transit protection does your data have?
- If you're not in the cloud, is it time to migrate?
- How will you orchestrate operations between two or more cloud deployments?
- What kinds of systems do you have in place to show how data moves throughout a hybrid or multi-cloud deployment?
- Where are your backup and disaster recovery systems located?
- If you need to move data out of a region, what are the implications with regard to data sovereignty?
- How will complying with data sovereignty impact your overall cost of operation?
- Who is responsible for meeting data sovereignty requirements in your organization?
- Can you use technology to help monitor your data?
- Can you report on the data that you own?

No matter where your data is stored, it's critical that you're aware of the particular data sovereignty laws your data is subject to. It's even more critical to understand these laws if your data spans more than one region with distinct data sovereignty.

This examination of some of the major data sovereignty laws around the world is just the beginning of your journey. The next step is to determine which laws apply to your deployments and what you need to do to respond to them.

Acronis

Learn more at
www.acronis.com