What is data sovereignty and how does it apply in the public cloud environment?

PAYMENT CONNECTIVITY ACCESS CONTROL IDENTITY TRAVEL JUSTICE & PUBLIC SAFETY

POSTED ON 03.21.23

Put simply, data sovereignty is about being in control of what matters, in terms of the laws and data protection regulations applicable to an organization's data at any or all phases of the data lifecycle. It's a very broad term that is incredibly important to grasp when applied to the public cloud environment. Why? Because data in the public cloud is hosted at a third party location, where various requirements define what data sovereignty actually means in this context.

It is crucial to note that while **data privacy** gets a lot of attention in the public debate and is a significant aspect of data sovereignty, it is not the only one—data sovereignty extends to **securing critical infrastructures** as well. For example, countries have sensitive data that they want to keep within their own country and therefore, under their control. This could be any information critical to the operation and management of critical infrastructure, such as a power grid, a telecom network or healthcare system.

Given the range of services that can benefit from being hosted in the public cloud environment and the various levels of sensitivity of the related data, there are **many ways to think about data sovereignty**. It can be broken down into three main areas: data residency, operational control and legal control.

Data residency, the most common way to think about data sovereignty

The majority of companies and countries use the terms data sovereignty and data residency interchangeably. Data residency relates **to where (the actual physical location) sensitive data is stored or processed**—often a country or region, or the physical location of a cluster of data centers where an application is deployed. The "where" is important because the location defines the applicable jurisdiction and impacts the level of control a country has over the data, process and operations.

Data residency is a **common expectation** across all sectors and is generally **easy to meet** for major public cloud service providers given the vastness of their global data center networks. Here, the public cloud environment is also clearly an advantage for companies operating in multiple jurisdictions because it allows them to store sensitive data across multiple data centers in several geographic regions around the world to **comply with local data protection regulations**.

Operational control: data sovereignty at the infrastructure level

The second most common element of data sovereignty is operational control and relates to **who manages the underlying infrastructure** that stores, processes and protects sensitive data and relevant applications. It is about defining controls and policies to determine **who can access information** and putting teams in place that can be trusted to secure sensitive data. Companies can implement various controls to verify who has their "hands on the keyboard." This can include:

- **auditing** in place to produce compliance artifacts;
- obtaining **certifications** to prove operational control or, more recently;
- implementing **technology solutions** such as confidential computing—which focuses on encrypting sensitive data when it is processed by a virtual machine—to ensure that no one, not even those with their "hands on the keyboard" can access the data in clear.

Legal control: the most stringent way to think about data sovereignty

The third, toughest and least common data sovereignty requirement is legal control. **When a state requests legal control, they're asking that the cloud service provider be within their own legal jurisdiction**, and thus beyond the jurisdiction of foreign powers. This means that the cloud service provider, who owns and manages assets, is not subject to foreign influence and cannot be compelled to comply with any foreign party.

When we consider that US-based companies currently account for more than 70% of the public cloud service provider market share, it is **clearly difficult for a non-US company or government** to expect legal control while also reaping all the benefits of the public cloud environment. That being said, very few entities require legal control today—**and when they do, it is for very specific workloads**.