Data Sovereignty, Residency and Localization in the Cloud

Compliance with Privacy and Data Protection Regulations in the Cloud

Guide

Forcepoint

Understanding Data Sovereignty, Residency and Localization in the Cloud

Forcepoint is committed to assisting our customers with staying compliant with their local and regional privacy and data protection requirements as we understand it can get complicated when it comes to choosing cloud services in today's global privacy and data protection regulatory landscape. It's important to understand your legal requirements when it comes to managing business and personal data so that you remain compliant with your local privacy and data protection laws.

Most cloud service providers (CSP) use a distributed cloud data processing infrastructure to provide their services to customers globally, so it is imperative to know what your local data protection laws require when it comes to transferring your local data outside of the country or legal jurisdiction that governs the legal requirements for the data.

Inevitably, the terms of data sovereignty, data residency, or data localization will come up when discussing the possibility of procuring services from a new CSP so make sure you clearly understand what each term means and how it may impact your ability to use certain cloud services. Most global privacy and data protection laws like the EU GDPR, UK Data Protection Act, Singapore's PDPA and India's new DPDP Act contain requirements for the transfer, processing and storage of personal data that are aligned with the definition of data sovereignty.

Data sovereignty is defined as the principle of ensuring that the data protection requirements, transfers, processing, and storage of data are compliant with and remains subject to the local laws of the country or region where the data is collected.

Data residency simply refers to the physical or geographic location of where data is stored. The term is often used to denote the country or region that the data is subject to when discussing data sovereignty requirements for the data itself. It does not mean that the data is bound to the physical location and cannot be transferred to another location, unless there are specific local legal requirements for certain data (e.g., financial records, critical government data, and/or sensitive personal data) to be localized in the country or region of data residency.

Data localization requires data to either (a) be stored and processed within the country or region it was collected, or (b) that a replica copy of certain data is physically stored locally within the boundaries of the country or region. Typically, data localization is only required for certain data that is specified under the law by the local government as being critical or sensitive information (e.g., financial records, critical government data, and/or sensitive personal data). China and Russia have some of the most restrictive data localization requirements that restrict the transfer of their citizen's personal data without direct government authorization.

To summarize, data sovereignty is focused on the ability to apply the local legal rights and protection requirements for the data in relation to the storage and processing of the data, data residency is the physical or geographic location of where data is stored, and data localization requires that either a copy of certain data or all data must to be stored and processed within the country or region it was collected.

Frequently Asked Questions

Question	Answer
What does data sovereignty, localization, and residency have to do with global data protection and privacy laws?	Global data protection and privacy laws often include provisions related to data sovereignty, localization, and residency. These laws regulate how data can be collected, stored, used, and transferred, and they can vary significantly from one country to another
Why are data sovereignty, localization, and residency important?	These concepts are important for legal compliance, data protection, business continuity, and maintaining control over data. They are important terms to be familiar before initiating cross-border data transfers and international data sharing agreements.
What is the difference between data sovereignty and data ownership?	While data sovereignty refers to the legal and regulatory control over data, data ownership refers to who has the rights to possess, use, and dispose of the data.
Who is responsible for ensuring compliance with data sovereignty, localization, and residency requirements?	Organizations that collect, store, or process data are responsible for ensuring compliance with these requirements. The organization that is the data owner and/or data controller is legally responsible for the compliance of their data. Typically, cloud service providers have a shared responsibility as a data processor to be compliant with the data controller's local data protection requirements.
Are Forcepoint products and services compliant with my local data sovereignty requirements?	Yes. Forcepoint products and services are compliant with data sovereignty laws and are designed with Privacy by Design in mind to allow the flexibility for our customers to configure the product and services to meet their local privacy and data protection requirements.
Is data residency essentially the same as data localization?	Not at all. Data residency is just a term to denote the physical or geographic location of where data is stored, whereas data localization means that there are local data protection and/or privacy laws that require that certain data must be stored and processed in the country or region where it was collected.
What if someone is telling me that data localization is required for their data?	It is important to understand the specific data that is subject to localization and if the requirement is to only retain a local copy of the subject data. • What is the local regulation that applies to the localization requirement? • Does it only apply to certain types of data?

	• Can the data still be transferred outside the country or region for storage and processing, if a local copy of the data is retained?
How can organizations ensure compliance with data sovereignty, localization, and residency requirements?	Organizations can ensure compliance by understanding the laws in the countries where they operate, implementing appropriate data management and protection measures, and regularly reviewing and updating their practices.
How can I learn more about how Forcepoint protects my privacy and data?	Visit the Forcepoint Trust Hub webpage at https://www.forcepoint.com/legal/forcepoint-trust-hub to learn about the Forcepoint Privacy Program and how our products protect your personal data in the Management of Personal Data product support documents.

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.