

Digital sovereignty and sovereign clouds

So far, you've learned that risk protection programs are an important part of mitigating risk, and stopping data breaches. Digital sovereignty and the sovereign cloud are also important concepts cloud security professionals should understand. In this reading, you'll learn about the sovereign cloud, and why many countries are concerned with digital sovereignty. Please note, the following reading should not be considered legal advice.

Sovereign clouds

Sovereign clouds are cloud architectures that operate in a particular country or region, and meet a governing body's legal data privacy standards. The primary reason for a sovereign cloud is to ensure that the laws of a country can be applied and enforced on the data processors and controllers that operate in that country.

Sovereignty can sometimes be related to national security. Information may need to remain on sovereign territory so that it cannot be accessed by another country. This often includes healthcare data. Many government bodies are adopting sovereign clouds that guarantee data is compliant with local privacy laws and standards.

Many countries are also seeking digital sovereignty for national security reasons, or to protect the data of private citizens. The downside of digital sovereignty is that it requires more effort and diligence, and can become costly for multinational organizations.

Sovereign clouds are created to connect the needs of both governments and private organizations. They allow countries to maintain data sovereignty, but also allow multinational organizations to stay competitive.

If an organization fails to meet the cloud sovereignty requirements of a country, they may be prohibited from operating their business in that country. This applies to the cloud service provider, and the companies using the cloud service.

Key takeaways

It's important to remember that sovereign clouds can help ensure that the data privacy laws of a country can be applied and enforced. Sovereign clouds are often desirable for national security reasons, because they can help prevent data and information from being accessed by other countries. Failure to comply with sovereignty requirements of a country can put an organization at risk for being prohibited to do business in that country.

Resources for more information

Check out this resource to learn more:

- Learn more about sovereignty and Google in [T-Systems Sovereign Cloud and Google Cloud](#).