Digital Sovereignty and How to Implement Sovereign Solutions

IDC

What Is Digital Sovereignty?

IDC defines digital sovereignty as the capacity for digital self-determination by nations, companies, or individuals. That means digital self-government where you have total control over all your data, including all the underlying infrastructure such as the datacenters, networks, and the support and admin personnel that have access.

What about Cloud Sovereignty?

As the foundation for digital business innovation, cloud will be at the core of digital sovereignty developments. Organizations seeking sovereign solutions will have to factor a sovereign cloud into their multicloud strategies, at least for certain workloads. IDC considers data sovereignty and cloud sovereignty to be subsets of digital sovereignty.

Why Is This Important Now?

Economic and geopolitical turmoil continue to impact organizations globally. IDC data shows that more than 80% of organizations now consider digital sovereignty to be a more important business and technology concern. It can provide the extra armor needed to boost resilience and security, not only for businesses but also at a national, governmental level to ensure the continued operation of critical infrastructure and systems.

IDC

86% of CEOs globally say Digital Sovereignty is their highest priority over the coming years, and that ranks alongside the need to address cybersecurity threats.

Sovereignty is not a game of Monopoly where dominance is the goal; the aim for vendors and their customers is to become stronger competitors on the global digital stage. Put another way, digital sovereignty gives data-driven organizations a license to operate.

How to Implement Sovereign Solutions

- Digital sovereignty, and in particular data sovereignty, can be mandated by national legislation or industry regulations, which means organizations will need to deploy sovereign solutions.
- But even if that is not the case, organizations should still consider digital sovereignty as a strategic priority. It may be required to gain access to an ecosystem of partners, and in addition there are still business benefits to be had by implementing solutions for digital sovereignty.
- Once an organization has decided to deploy such solutions, there are two crucial first steps:
  - Carry out a review of what is needed for sovereignty, and then classify your data because not all workloads will need to be migrated to a sovereign solution.
  - Once that's done, organizations should use regulatory and legal frameworks to stay on the right side of the data protection officers, and everything should be supported by dedicated APIs.
- Sovereignty solutions are, by their very nature, restrictive, so you've also got to make sure you keep everything in balance so as not to stifle innovation. Partnerships between global and local providers are vital here.
- The final part of the process is to maintain security and compliance on an ongoing basis. Crucially, this must be a shared responsibility between all partners — sovereignty success is based on working within an ecosystem.

IDC

Many of the steps here — such as reviewing security, classifying data and apps according to workloads, maintaining security on an ongoing basis — are really part of best practice and due diligence processes that are, or should have been, on the enterprise IT agenda from the outset.

While there are plenty of examples of data protection authorities around the world handing down multimillion-dollar fines to organizations that have breached local data privacy laws, there's no legislation as such that covers digital sovereignty. However, countries such as Austria, France, and the Netherlands have ruled that the use of a default setup of Google Analytics, where personal information is moved from Europe to Google servers located in the U.S., is in breach of GDPR rules on data transfers. And in Germany, the lead data protection authority has determined that Zoom's data transfers to the U.S. are also in violation of GDPR and has issued a formal warning to members of the state government to stop using the platform.

IDC

Business Benefits

71% agree that implementing digital sovereignty prevents unfair competition in digital markets and encourages rules-based partner cooperation within ecosystems.

78% believe it improves their ability to shape digital transformation efforts in a self-determined way.

76% of organizations around the world say digital sovereignty enhances customer, government, and stakeholder trust in their operations and businesses, and can therefore open access to new global markets.

44% of organizations globally believe the top business benefit of using sovereign cloud solutions is a stronger security posture.

IDC

For more information

What is digital sovereignty? And why is it important? Watch IDC's global Digital Sovereignty lea,d Rahiel Nasir, define the concept, explain the pitfalls to avoid, and offer key recommendations to those offering solutions.

You can find more information on Digital Sovereignty and cloud trends in our European Cloud Trends webcast from earlier in the year.

To learn more about IDC's Digital Sovereignty research, contact your account representative or check here.