Google Cloud

Author: Cheryl Scully
Contributors: Wilfried Teiken, Dwight Worley, Senanu Aggor, Lorrie Ma, Sean Osterberg

Digital Sovereignty on Public Cloud

Google Cloud Data Boundary



Table of contents

01
Executive Summary 03

02
Background 04

03
What is digital sovereignty? 05

04
Google Cloud's approach to digital sovereignty 05

05
What is the Google Cloud Data Boundary? 06

06
Key controls and capabilities 07

07
Additional controls 08

08
How the Data Boundary provides digital sovereignty 09

Case study 10

The Solution 11

Outcome 12

09
Take the next step 13



Executive Summary

Google Cloud is committed to creating products that enable organizations with strict sovereign data requirements to build secure and innovative solutions. Our product portfolio — recognized for leading in the sovereign space — gives our customers ownership and control of their data, operations, and software. Our verifiable, zero-trust framework lets customers maintain strict compliance with data protection laws globally, digitally transform their operations with all modern cloud capabilities, including generative artificial intelligence, and unlock significant market opportunities with complete peace of mind.

This white paper explains how Google Cloud helps governments and regulated firms overcome data sovereignty and compliance challenges that traditionally restrict them to on-premises or legacy GovCloud solutions. With a comprehensive Sovereign Cloud portfolio, anchored by Google Cloud Data Boundary via Assured Workloads, customers can enforce data residency, limit extraterritorial data access, and eliminate the expensive operational burden of maintaining continuous compliance on-premises.

Google Cloud eliminates the trade-off between sovereignty and innovation, offering verifiable, zero-trust controls —including Data Residency, Customer-managed Encryption Keys (CMEK), and Key Access Justifications (KAJ)—for sensitive data, providing unmatched public cloud transparency.

This white paper explains how Google Cloud helps governments and regulated firms overcome data sovereignty and compliance challenges.

Background

Governments and regulated sectors are focused on technology innovation while also ensuring that data remains compliant, secure, and private.

In this increasingly complex environment, the growing global demand for compliance solutions is driven by three main factors:

01

Regulations: Organizations need more digital and physical control over their data and operations to comply with local laws and industry-specific regulations.

02

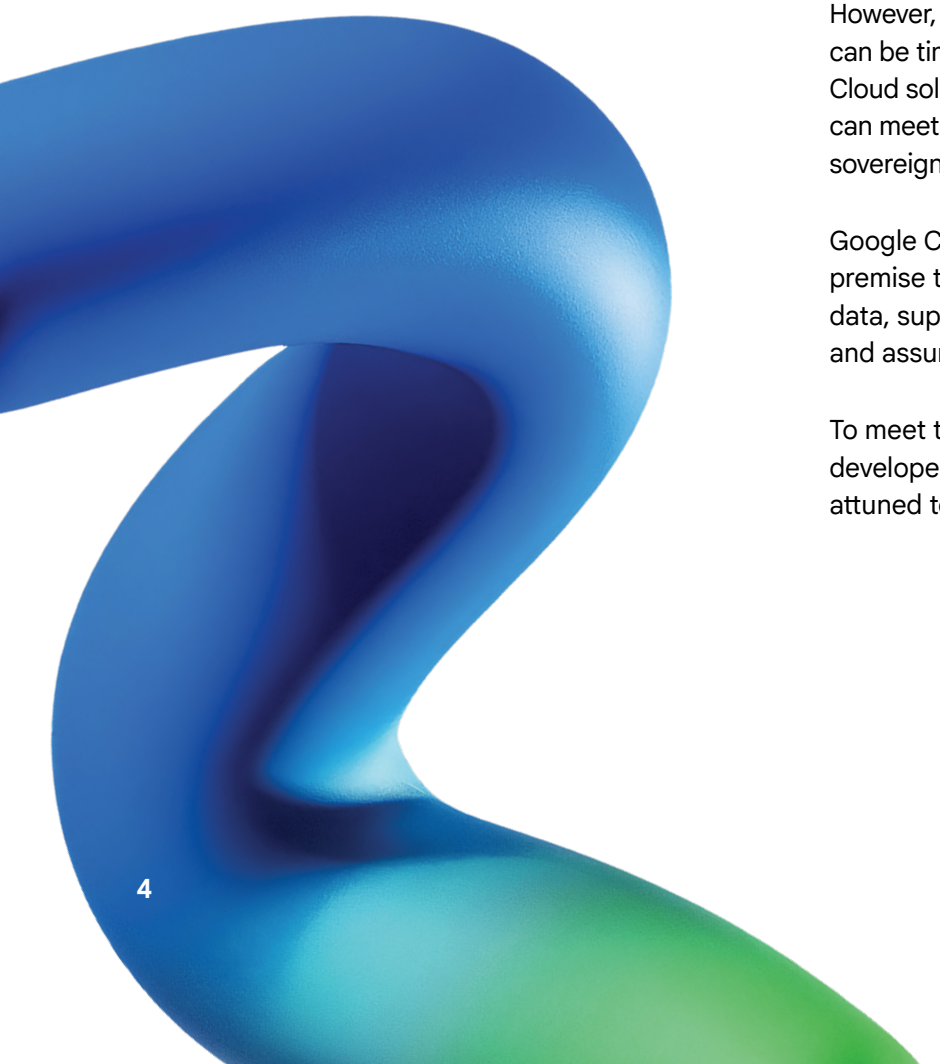
Geopolitical evolutions: Organizations must ensure that their data and operations are resilient against emerging global challenges.

03

Need for faster innovation: External pressures require faster innovation and transformation. However, developing these capabilities in-house can be time-consuming and expensive. Cloud solutions and cloud-based services can meet this need, but they must include sovereign guarantees for compliant adoption.

Google Cloud operates on the fundamental premise that customers own and control their data, supported by foundational Trust Principles and assurances of transparency and oversight.

To meet these compliance needs, Google developed several sovereign solutions, attuned to each jurisdiction's requirements.



What is digital sovereignty?

Digital Sovereignty is about control — over location, encryption, software, and access to your customer data. These principles include:

Data Sovereignty: Customers can control the encryption and location of their data (in transit and at rest), restrict access, restrict the deployment of non compliant resources, and limit support personnel access based on predefined attributes.

Operational Sovereignty: Operations performed by a local third-party operator or customers have visibility over Google operations.

Software Sovereignty: Customers can run their own workloads without dependence on the provider's software, letting them control the software they use.

Google Cloud's approach to digital sovereignty

These principles are achieved through a comprehensive Sovereign Cloud portfolio—spanning **Google Cloud Data Boundary** for data residency and access control on the public cloud, **Google Cloud Dedicated** for use cases requiring data center ownership and operation by a local partner, and **Google Cloud Air-Gapped** for environments with the strictest requirements.

Google Cloud Data Boundary via Assured Workloads is the public cloud framework that provides customers with required control over data location, access, and encryption, and accountability through auditable logs. This framework is also a safeguard against erroneous configurations that would misplace or expose data.



Our Sovereign Cloud products are designed to meet diverse regulatory landscapes, geopolitical dynamics, and innovation needs (Figure 1). We provide tailored control precisely where our customers require it, ensuring they can confidently navigate their path to sovereignty while retaining full cloud capability and agility.

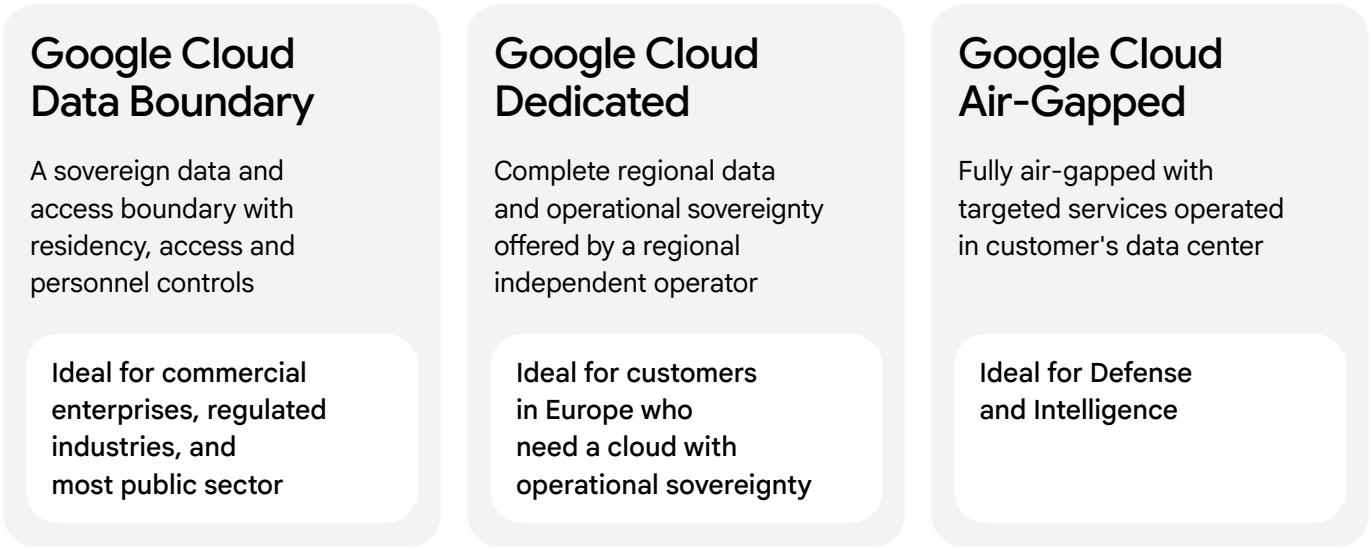


Fig 1. Google Cloud's data sovereignty portfolio

Google Cloud provides sovereignty offerings around the world, with commitments outlined in our Service Specific Terms and resources such as Trusting your Data on Google Cloud.

What is the Google Cloud Data Boundary?

Google Cloud Data Boundary is a layer of software controls on the public Google Cloud that empower customers to leverage Google's innovation and scalability while retaining control over data location, transparency into administrative actions, and cryptographic keys protecting their data. Customers can access a large set of Google Cloud products, including AI services (on supported solutions), and can choose control frameworks with increasing levels of controls.

Data Boundary solutions span Google Cloud regions and jurisdictions, regulatory packages, and Data Boundary by Partners.



Key controls and capabilities

Google Cloud Data Boundary leverages software-defined technical controls for in-depth defense, local partners for an additional layer of sovereignty, and Shared Fate and transparency models. The following controls, while available a la carte in Google Cloud, are preconfigured with organization policies and standardized packages via Data Boundary. They are attuned to the region in which the package is offered (whether the EU, Canada, or elsewhere), only utilizing services and features that support controls as required for compliance.

Data Residency: Lets users specify that customer data at rest and in process, and new resources, are created and stored in a particular geographic region or jurisdiction.

Encryption and Key Management: Data is encrypted by default, both in transit and at rest. Optionally, customers can use **Cloud Key Management Service (KMS)**, which lets them manage their own encryption keys, a process known as **Customer-Managed Encryption Keys (CMEK)**.

Transparency and Auditing: Most Data Boundary solutions provide Access Transparency logs, letting customers review what accesses were made by Google staff, and why.

Access Approval lets customers require explicit approval for any access to their data by Google personnel.

Assured Support: A value-added service to Premium or Enhanced Support to ensure only Google support personnel meeting specific geographical locations and personnel conditions support their workload when raising a support case or needing technical assistance. (Available for select control packages)

Employee Access Safeguards: Google uses a "zero trust"-based architecture and "least privilege" principles to protect data from internal access. Access is monitored continuously, and unusual events are investigated by dedicated security teams.

Compliance and Certifications: Google Cloud undergoes regular, independent third-party audits and certifications to verify its data protection practices. Data Boundary via Assured Workloads is built upon Google Cloud's foundation of internationally recognized standard certifications, including ISO 27001, SOC 2/3, GDPR and PCI DSS.

For customers who need stricter sovereign control, Google Cloud offers packages with additional value-add features for more sensitive data needs:

Cloud External Key Manager **(Cloud EKM)** lets customers store and manage keys outside of Google's infrastructure. With Cloud EKM, customers can also leverage Key Access Justifications to control keys based on clear and precise justifications.

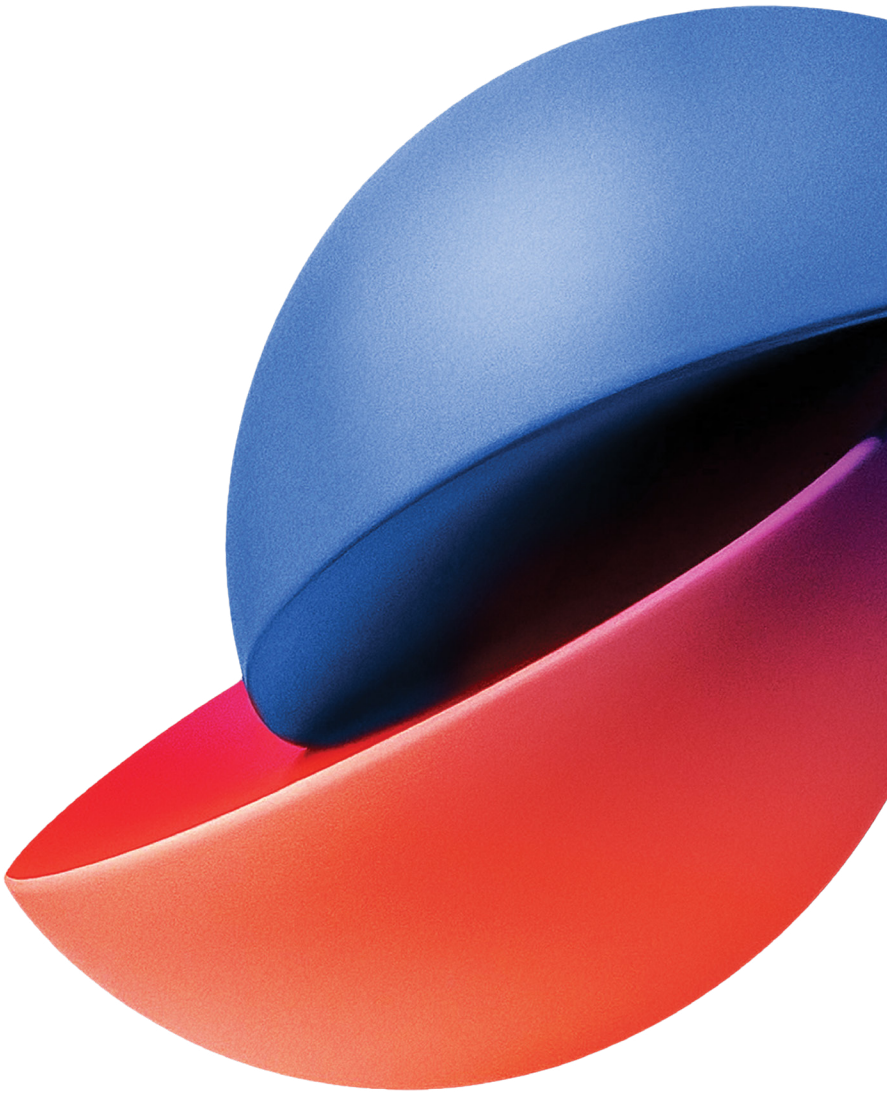
Key Access Justifications empowers customers to exercise zero trust control over Cloud EKM key, ensuring that sensitive data and workloads cannot be decrypted without the informed consent of a customer-configured system outside of Google. Key Access Justifications, paired with Google's commitment to be truthful and transparent on any access request provenance, differentiates Google Cloud from other hyperscalers.

Trusted Sovereign Partner: Through the **Data Boundary by Partners** solution, a local, trusted partner can provide third-party oversight of Google administration, local contracting, and management of EKMs and Key Access Justification policy.

Additional controls

VPC Service Controls: Restricts network locations from which users can access data, even if they are otherwise authorized.

Confidential Computing: Encrypts data while it is being processed in a virtual machine's memory and can be optionally integrated with Data Boundary solutions.



How the Data Boundary provides digital sovereignty

Digital Sovereignty is addressed by either Regional / Jurisdictional or Regulatory Data Boundary solutions. Customers who require data residency in a specific region or jurisdiction, with optional controls such as CMEK, administrative access justifications, and regional / adjudicated support, choose Regional data boundaries. Customers adhering to a specific regulatory framework, such as Canada Protected B or HiPAA, choose one of our Regulatory data boundary solutions.



Google Cloud goes beyond the offerings of other hyperscalers by providing **technical controls to reinforce legal protections** against unauthorized access to customer data, outlined in the white paper Government Requests for Cloud Customer Data.

Google publishes the Google Transparency Report, where we share information about how the policies and actions of governments and corporations affect privacy, security, and access to information.

Additionally, Google differentiates itself by establishing sovereign solutions with local partners within **Data Boundary by Partners**, who provide local contracting, offsite key operations, and oversight of administrative access and software versioning. Sovereign partners provide third party assurances for our customers, entering into a three-way Shared Fate partnership underpinned by transparency, allowing customers to harness the power and innovation of cloud with the safety of third party protection.



Case study: European telecom provider ensures data sovereignty and innovation

A major European telecommunications provider was grappling with a fundamental challenge: how to modernize its core business operations and leverage advanced cloud capabilities, including data analytics and AI, while strictly adhering to national data sovereignty laws and protecting vast amounts of customer Personally Identifiable Information (PII).

The company's primary concerns were:

01

Data Residency: Ensuring all customer PII remained physically and legally within the country's borders.

02

Administrative Access Control: Maintaining verifiable oversight and control over any necessary access by the cloud provider's (Google Cloud) administrative personnel.

03

Cryptographic Control: Possessing "veto power" over data decryption to prevent unauthorized extraterritorial access.

The Solution: Google Cloud Data Boundary by Partners

To resolve the sovereignty-vs-innovation trade-off, the telecom provider chose the **Google Cloud Data Boundary by Partner** solution. This framework allowed them to leverage the full scalability and security of the Google Cloud public platform while implementing a robust, verifiable zero-trust control set managed in partnership with a local, trusted sovereign partner.

The solution was built on three foundational pillars:

Control mechanism	Description	Benefit to the customer
Data Residency	Google Cloud's data boundary policies were configured to enforce strict geographic residency, ensuring customer PII at rest and in transit never left the designated European region.	Guaranteed compliance with local data protection laws, eliminating the risk of accidental jurisdictional breach.
Trusted Sovereign Partner Oversight	A local, trusted partner provided administrative oversight and was the primary contracting party for key security controls.	Ensured local governance and accountability. The partner had full transparency into, and veto power over, Google administrative access requests via Access Approval and Key Access Justifications.
External Key Manager (EKM) and Key Access Justifications (KAJ)	The encryption keys for the customer's most sensitive data were stored and managed in an EKM operated by the sovereign partner, outside of Google Cloud's infrastructure. Every key access request from Google Cloud was automatically routed for partner approval via KAJ.	Provided the highest level of cryptographic control. The partner could instantly deny any decryption request that lacked a valid business justification or originated from an unauthorized jurisdiction, ensuring a "fail-closed" mechanism for the PII.



Outcome

By deploying Data Boundary by Partner, the telecom achieved:

Auditable sovereignty: All customer PII was verifiably protected by regional residency, local partner oversight, and customer-controlled encryption keys, satisfying stringent national regulatory requirements.

Accelerated innovation: By leveraging Data Boundary software controls atop the public cloud, the company rapidly adopted Google Cloud's data analytics and other services on their newly secured platform, leading to faster product launches, enhanced customer service, and significant operational cost savings.

Data Boundary by Partner provided the verifiable proof of control and zero-trust assurance the telecom needed, transforming a compliance bottleneck into a competitive advantage.

Take the next step

By providing granular control over data location and encryption — and transparency over administrative access, optionally augmented by local partner oversight — Google Cloud enables governments and regulated enterprises to confidently modernize, embrace cutting-edge cloud services like AI, and maintain absolute digital sovereignty.

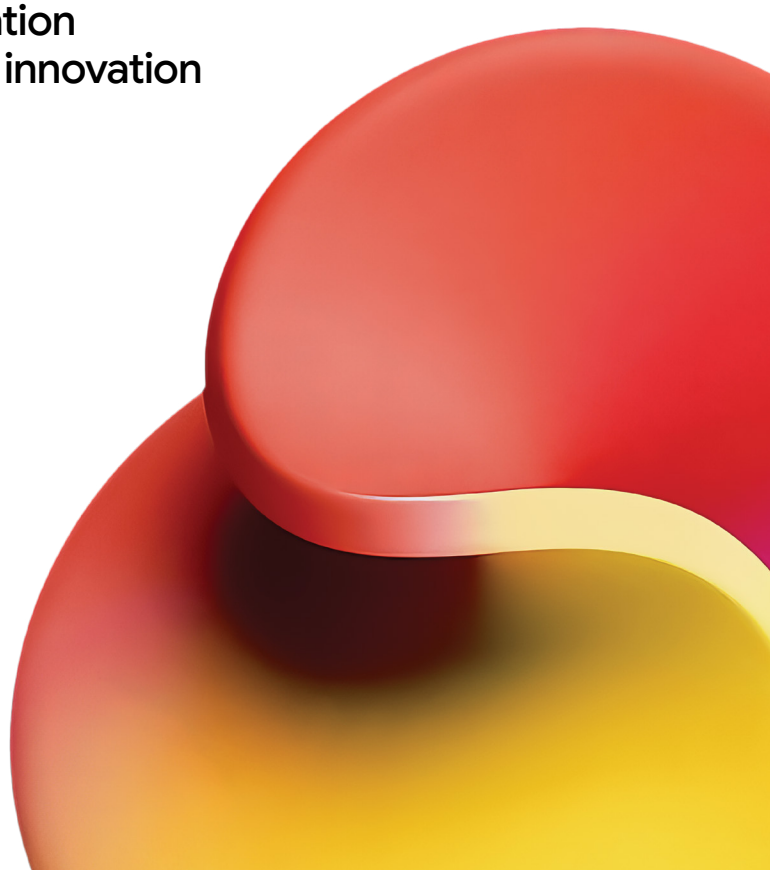
Are you ready to eliminate the trade-off between strict data sovereignty and rapid cloud innovation?

Contact your Google Cloud representative today to discuss how Data Boundary can be tailored to meet your organization's specific compliance, geopolitical, and innovation requirements.

Explore the Sovereignty Explorer to find the Google Cloud Data Boundary solution that aligns with your regional or regulatory needs.

Request a detailed consultation to understand the verifiable zero-trust controls and how they provide unmatched control and transparency for your most sensitive data.

Start your compliant digital transformation journey with Google Cloud and unlock innovation with absolute confidence and control.





Google Cloud