

Strengthen digital and data sovereignty

Avoid difficult tradeoffs between jurisdictional control and security, performance, and reliability

Need

Companies and governments around the world want greater control over their data and stronger resilience across their tech stacks. As a part of this trend, some organizations are evaluating their dependency on foreign technology service providers — particularly through the lenses of service continuity, government access to data, and operational data access within providers themselves.

Unfortunately, two common obstacles complicate sovereignty initiatives:

- Official sovereignty frameworks are still being developed by governments, regulators, and private industry, leaving many organizations unsure of where to focus their efforts.
- The distributed nature of modern network infrastructure and cloud environments mean that stronger jurisdictional control can cause tradeoffs with security, reliability, and performance — not to mention operational complexity and cost.



How Cloudflare can help

Cloudflare helps organizations enforce jurisdictional control over data and boost tech stack resilience while still benefiting from the security, scale, and operational efficiency of our [connectivity cloud](#):



App delivery

Limit caching, decryption, and traffic processing to specific regions, while still mitigating DDoS attacks with global scale.



SASE

Enforce a variety of data locality rules. Make your remote access more resilient with easy failover options.



Developer services

Control the countries and regions serverless compute takes place in. Choose from a variety of sovereign and global AI models.

How it works

Sovereignty is a principle and a right, not a capability you can buy. As such, Cloudflare's sovereignty approach blends technical controls with a sovereignty-forward governance posture and support for broader resiliency and interoperability.

Technical controls

Cloudflare's sovereignty-supporting services and flexible architecture let customers enforce jurisdiction-configurable data sovereignty controls across our product portfolio.

- **Data inspection:** Limit caching, inspection, decryption, serverless compute, and more to specific countries or regions — while still blocking DDoS attacks with global scale.
- **Encryption:** Store TLS private keys in your own sovereign data center. Protect user and customer traffic with quantum-resistant encryption.
- **Logging:** Send Cloudflare logs to a sovereign data center. Ensure end-user metadata doesn't leave the EU or US.
- **Privacy:** [Protocols](#), [proxies](#), [user authentication](#), and [analytics](#) that hide end-user data from Cloudflare altogether.

Broader sovereignty support

Cloudflare's resilient, interoperable architecture helps organizations reduce dependencies on individual technology providers:

- Failover and exit options for our app delivery, SASE, and developer services.
- Run the AI models of your choice
- Manage connectivity and security across sovereign and global cloud providers.



Governance posture

Cloudflare reinforces our technical sovereignty capabilities with legal transparency and due process commitments:

- Official policy and strong history of challenging unreasonable legal demands, defending data privacy, and resisting restrictions to service availability.
- [Public commitments](#) about actions we will never take in response to government demands.
- Responses to government requests are recorded in our [Transparency Report](#).

Doctolib

"The Data Localisation Suite is invaluable for us because it allows us to use Cloudflare while remaining compliant. And no one else in Europe has Cloudflare's capabilities and ability to handle the massive amount of traffic we have."

- **Cédric Voisin**
CISO

Customer stories



REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

Estonia's Information Security Authority uses Cloudflare to boost web resiliency and control data locality.

- The **Data Localization Suite** ensures that Layer 7 data is only processed in EU and EEA-based data centers
- **DDoS Mitigation**, **Bot Management**, and **Rate Limiting** keep web applications from being overwhelmed by traffic



The world's most popular female health app uses Cloudflare to anonymize sensitive data and secure internal application access.

- **Privacy Gateway** lets Cloudflare serve application traffic without being able to link user identities with request content
- **SASE services** let Flo enforce Zero Trust, device context-aware access policies for all internal applications

Learn more about Cloudflare's sovereignty approach



[Learn about the Data Localisation Suite](#)



[Read our most recent Transparency Report](#)



[Talk to our team about your sovereignty needs](#)

