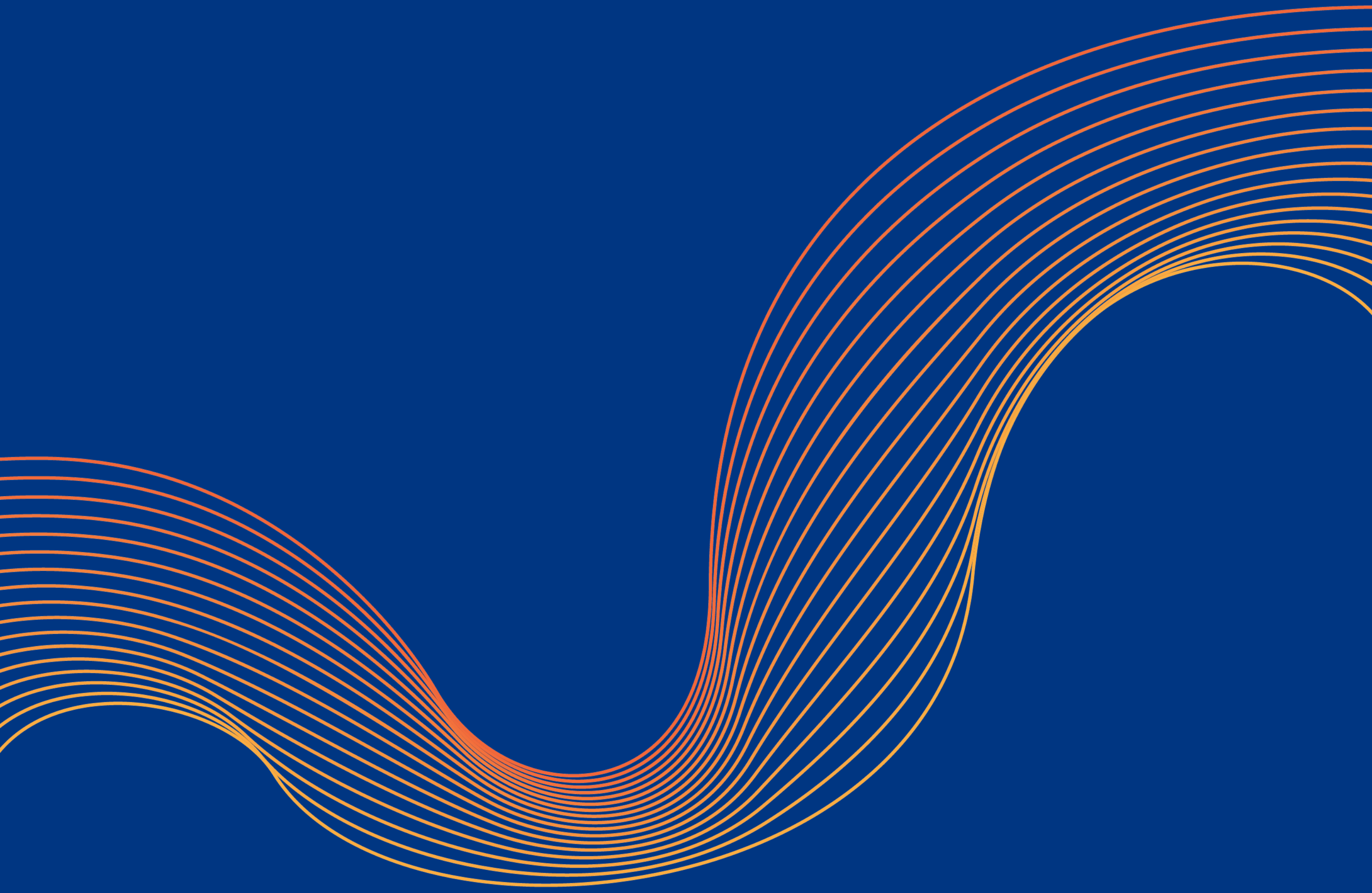
CLOUDFLARE®

How Cloudflare localises data in the EU



1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

Introduction

Cloudflare is committed to helping our customers comply with their obligations to keep personal data in the EU.

That is why Cloudflare offers our Data Localisation Suite, which is a set of products that give customers control over where their data is inspected and stored. In this document, we'll cover the technical aspects of the Data Localisation Suite to explain how data stays local.

The Data Localisation Suite helps customers with three distinct areas:

1. **Encryption Key Management** (Geo Key Manager and Keyless SSL)
2. **Payload Inspection Boundary** (Regional Services)
3. **Customer Metadata Boundary**

Encryption Key Management

Customers may choose to use either Keyless SSL or Geo Key Manager to ensure that their TLS keys do not leave the EU.

Keyless SSL

With Keyless SSL, organizations are able to leverage Cloudflare while maintaining custody of their key material. Keyless SSL is a good fit for customers that want to use their own keyserver and Hardware Security Module (HSM). Keyless SSL is only "keyless" from Cloudflare's point of view: Cloudflare never sees the customer's private key, but the customer still has and uses it. Meanwhile, the public key is still used on the client side like normal.

SSL, more accurately known as TLS, is a protocol for authenticating and encrypting communications over a network. SSL/TLS requires the use of what's called a public key and a private key. When a company uses a vendor like Cloudflare, the vendor typically has access to the private key in order to provide services like WAF and caching. Keyless SSL allows Cloudflare to work, while ensuring the private key remains securely in the customer's possession.

Keyless SSL relies on the fact that there is only one time when the private key is used during the TLS handshake, which occurs at the beginning of a TLS communication session. Keyless SSL works by splitting the steps of the TLS handshake up. Keyless SSL moves the private key part of the process to another server, usually a server that the customer keeps on premises. Instead of using the private key directly to generate session keys, Cloudflare gets the session keys from the customer over a secure channel and uses those keys to maintain encryption. Thus, a private key is still used, but it is not shared with anyone outside the customer's company.

For instance, suppose that Acme Co. implements SSL. Acme Co. will securely store their private key on a server that they own and control. If Acme Co. begins using Cloudflare with our default SSL option, Cloudflare will then have the private key. However, if Acme Co. starts using Keyless SSL, the private key can stay on the server that Acme Co. owns and controls, as in the non-cloud SSL implementation.

For even more technical details, please see our learning center

Geo Key Manager

Geo Key Manager is a good fit for customers who want to ensure their SSL keys stay in one region, but don't want to host their own key server.

Geo Key Manager uses Keyless SSL under the hood. Instead of having a customer run a key server inside their own infrastructure, Cloudflare can host key servers in just the EU. This reduces the complexity of deploying Keyless SSL, while still ensuring that private keys never leave the EU.

For even more details about how Geo Key Manager works, please see this article.

Payload Inspection Boundary

Regional Services

Keyless SSL and Geo Key Manager ensure that private key material does not leave the EU. Regional Services ensures that those keys are only used inside the EU. With Regional Services, TLS connections are only terminated in the EU. This means that Cloudflare will only be able to decrypt and inspect the content of HTTP traffic inside the EU.

When Regional Services is used, all of our edge "application services" will run inside the EU. This includes:

- Storing and retrieving content from Cache
- Blocking malicious HTTP payloads with the Web Application Firewall (WAF)
- Detecting and blocking suspicious activity with Bot Management
- Running Workers scripts
- Load Balancing traffic to the best origin servers

You can read more about Regional Services in this article.

Customer Metadata Boundary

What is Customer Metadata?

Cloudflare collects metadata about the usage of our products for the purposes of:

- Serving analytics via our dashboards and APIs
- Sharing raw logs with customers
- Stopping security threats such as Bots or DDoS attacks
- Improving the performance of our network
- Maintaining the reliability and resiliency of our network

Cloudflare's edge network consists of dozens of services: our Firewall, Cache, DNS Resolver, DDoS protection systems, Workers runtime, and more. Each of these services emit structured log messages, which contain fields like timestamps, information about the Cloudflare features used, and which customer the traffic belongs to. These messages are sent back to one of our core data centers for processing.

These messages do not contain the contents of customer traffic, and so they do not contain usernames, passwords, personal information, and other private details of customers' end users. However, these logs may contain end-user IP addresses, which is considered personal data in the EU.

Customer Metadata Boundary

The Customer Metadata Boundary ensures, simply, that all of the traffic metadata that can identify a customer stays in the EU. This covers all data for which Cloudflare is a processor (as defined in our Privacy Policy) and includes all of the logs and analytics that a customer sees.

All of the traffic metadata that can identify a customer flows through a component at our edge called "logfwdr" (pronounced "log forwarder"). Services that run at our edge send structured log messages to logfwdr, which batches and "forwards" logs to a core data center.

When the Metadata Boundary is enabled for a customer, logfwdr ensures that any log message that identifies that customer (i.e. contains that customer's Account ID) is not sent outside the EU. It will only be sent to our core data center in Luxembourg, and not our core data center in the U.S.

Conclusion

At Cloudflare, our mission is to help build a better Internet, and we believe the protection of our customers' and their end users' data is fundamental to this mission.

The Data Localisation Suite with its various products as described within this document helps businesses get the performance and security benefits of Cloudflare's global network, while making it easy to set rules and controls at the edge about where their data is stored and protected.