WHITEPAPER

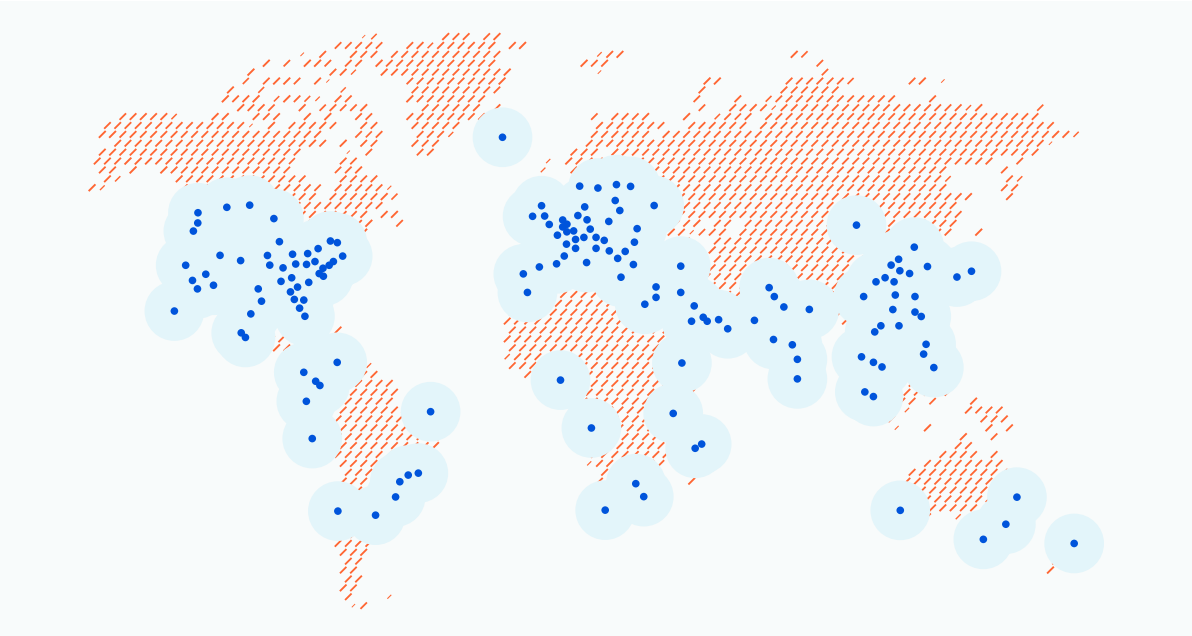
CLOUDFLARE

How Cloudflare helps address data protection and locality obligations in Europe

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

EXECUTIVE SUMMARY

- Cloudflare was built to help you and your end users be more secure on the Internet. We are a privacy-first company, and our network and all of our products are built with data protection in mind.
- Cloudflare maintains a broad set of legal and contractual protections that comply with the EU's GDPR.
- Cloudflare offers a suite of product features and technical protections for Cloudflare customers who do not want their data to leave Europe.



Cloudflare's unique global cloud network consists of data centers in over 250 cities across more than 100 countries. Cloudflare provides you with tools to manage how your data is routed through these data center so you can customize where your traffic is inspected in ways that meet your security, privacy, and performance needs.

About Cloudflare

Cloudflare's mission is to help build a better Internet. We provide a global cloud platform that delivers a broad range of network services to individuals and businesses of all sizes around the world. Cloudflare's network and growing portfolio of products improve the security, privacy, performance, and reliability of anything that is connected to the Internet. In addition to serving our customers, Cloudflare's mission is also to help make the Internet itself better — always on, always fast, always secure, always private, and available to everyone.

Cloudflare's network, developer community, and business are all ultimately built on customer trust. We seek to continually earn and maintain customer trust by being clear about our commitments to data privacy and how we manage customer and end user data on our systems. We also build trust by building and deploying products that (i) help improve the security of our systems, (ii) encrypt data at rest or in transit, and (iii) allow our customers to determine how traffic is inspected in different locations around the world. Finally, we earn customer trust by securing and maintaining industry-defined certifications (e.g. ISO 27001 and 27701, SSAE 18, and SOC 2 Type II) and providing contracting mechanisms (e.g. Data Processing Agreements) that communicate our shared responsibility model with our customers in ensuring privacy.

Cloudflare in Europe

Today, millions of global Internet properties use Cloudflare. This list includes many of Europe's largest and fastest-growing companies, including Eurovision, L'Oreal, AO.com, C&A, AllSaints, and many more well-known brands. It also includes a growing list of Europe's important institutions, including INSEAD, Börse Stuttgart, IATA, and Telefonica. As companies and organizations of

all sizes rely more on the Internet as a critical platform to serve their customers, users, and stakeholders, they are rapidly adopting secure and reliable cloud networks like Cloudflare to help protect their Internet-facing applications, infrastructure, and people from threats of all kinds.

We recognize that data protection in Europe presents unique challenges. Some of these challenges stem from the European Union's General Data Protection Regulation (GDPR) and the Court of Justice of the European Union's decision in the "Schrems II" case (Case C-311/18, Data Protection Commissioner v Facebook Ireland and Maximillian Schrems) — the latter of which resulted in further requirements for companies that transfer personal data outside the EU. In addition, a number of highly regulated industries require that specific types of personal data stay within the EU's borders.

As such, Cloudflare's Internet platform is built to support Europe's most privacy-conscious and regulated industries, including financial services, the public sector, energy, utilities, retail, gaming, and healthcare. At Cloudflare, we build our products to meet the highest standards of security and user privacy, and we partner closely with each of our European customers to help them meet data protection obligations associated with their specific location and industry segment. We accomplish this through a variety of avenues, including:

- Our overarching corporate commitment to privacy
- Maintaining global and European security certifications
- Maintaining GDPR-compliant data transfer mechanisms
- Offering product features which support data localisation

This paper explains those avenues in detail.

Cloudflare's unique corporate commitment to privacy

Cloudflare was built to help you and your customers be more secure on the Internet. We are a privacy-first company, and our network and all of our products are built with data protection in mind. We commit in our Privacy Policy that we will not sell personal data we process on your behalf or use it for any purpose other than to provide our services to you. Throughout our history, we've never violated this promise. In fact, our privacy stance was defined long before governments started regulating privacy in ways that forced many other technology companies to update their practices in order to appropriately prioritize customer and user privacy. We do not generate revenue from advertising — or profile our customers' end users or end-user data for any purpose — and thus default against the collection and retention of personal data we process on your behalf.

Below are some of the privacy commitments we make that differentiate us from many other cloud services providers:

- Cloudflare does not sell personal data.
- Cloudflare does not track our customers' end users across Internet properties.
- Cloudflare does not profile our customers' end users to sell advertisements.
- Cloudflare only retains personal data as necessary to provide Cloudflare offerings to our customers.
- Cloudflare has never provided to any third party or government our customers' encryption keys or a feed of customer content transiting our network, and we have a longstanding commitment that we would exhaust all legal remedies before complying with such a request.
- Cloudflare has publicly committed that we will pursue legal remedies to contest any U.S. government request for data that we identify as being subject to GDPR.

- Cloudflare's policy is to notify our customers of any legal process requesting their information before disclosure of that information, unless legally prohibited.

Cloudflare's global and European security certifications

Cloudflare meets industry-leading standards for security and privacy, and validates those commitments with third party auditors on an annual basis.

Cloudflare has been certified to a new international privacy standard for protecting and managing the processing of personal data — ISO/IEC 27701:2019. This standard is less than two years old, and adapts the existing Information Security Management System concept into the creation of a Privacy Information Management System (PIMS). There are requirements to make sure this privacy management system is robust and is also continually improving to meet its defined objectives. The standard is designed such that the requirements organizations must meet to become certified are very closely aligned to the requirements in the GDPR.

Put simply, the ISO 27701 certification provides assurance to our customers that we have a privacy program that has been assessed by a third party to meet an international industry standard aligned to the GDPR, and that requires us to keep our privacy program under continuous compliance. This certification, in addition to the Data Processing Addendum (DPA) we make available to our customers in the dashboard, offers our customers multiple layers of assurance that any personal data that Cloudflare processes will be handled in a way that meets the GDPR's requirements.

In addition, Cloudflare is compliant with ISO 27001/27002, Payment Card Industry Data Security Standards (PCI DSS), and SSAE 18 SOC 2 Type II. These validations provide assurance to organizations who transfer their most sensitive data through our services, and also help them meet and maintain their own compliance obligations.

In addition to the regular third-party assessments against industry standards, Cloudflare is considered an 'Operator of Essential Services' under the EU Directive on Security of Network and Information Systems (NIS Directive). As well as registering under this directive with the ICO and Ofcom in the United Kingdom, BSI in Germany, and CNCS in Portugal, Cloudflare has also been assessed against specific regional requirements, such as the BSI Act in Germany (BSIG). We embrace our relationships with, and work closely with, European regional regulators on compliance, and provide insights on how we are addressing data protection requirements.

On a practical level, the GDPR was a codification of many of the steps we were already taking:

- Cloudflare only collects the personal data we need to provide the service we're offering
- Cloudflare does not sell personal information
- Cloudflare gives people the ability to access, correct, or delete their personal information
- Consistent with our role as a data processor, Cloudflare gives customers control over the information that, for example, is cached on our content delivery network (CDN), stored in Workers Key Value Store, or captured by our web application firewall (WAF)

You can read more about our commitment to the GDPR here:

https://www.cloudflare.com/trust-hub/gdpr/.

Because we care about data protection, we do not just audit where we are required to do so by law or where certifications are available. Our security team performs rigorous internal and external penetration tests, we operate a bug bounty program through HackerOne, and we retain third-party auditors to validate our privacy commitments. Examples include our privacy-focused audits, like one we conducted in relation to our commitments for our 1.1.1.1 public DNS resolver. We are always open to obtaining additional validations that will provide assurance into our privacy program, policies, and practices for processing and storing EU personal data.

The data Cloudflare processes

Cloudflare processes the log data of our customers' end users when those end users access our services in line with our customers' authorization. This log data may include but is not limited to IP addresses, system configuration information, and other information about traffic to and from our customers' websites, devices, applications, and/or networks. In addition, Cloudflare collects and stores server and network activity data and logs in the course of operating our products, and makes observations and analysis of traffic data. Our Privacy Policy more specifically describes the information we collect and how we use collected information.

When we do collect and store data from activity on our network, we do so only to make our products better for you, for our other customers, or for the broader Internet community. We do not seek to monetize this data in any way we think would surprise you. For example, we may temporarily store and analyze network traffic data from all of our global customers so that we can intelligently route requests through the most efficient Internet paths. We may also store and analyze network data to detect and identify emerging threat vectors we can immediately use to improve our security tools. Finally, we may aggregate network data from significantly large customer segments (but never from individually identifiable users or customers) to help the Internet community understand trends and threats across the Internet (see Cloudflare Radar).

Cloudflare's data transfer mechanisms

In the event that Cloudflare, as a data processor, transfers personal data outside the EU, we do so under our standard Data Processing Agreement (DPA), which is incorporated into our Enterprise Service Agreement as well as our Self Serve Subscription Agreement. Our DPA incorporates the EU Standard Contractual Clauses (SCCs) (as updated in 2021) for data subject to the GDPR. Taken together, Cloudflare's terms ensure a level of protection for personal data equivalent to that guaranteed under the GDPR. You can find more information about our commitment to the GDPR and about our DPA here.

Under the Schrems II decision, EU-approved SCCs remain a valid transfer mechanism under GDPR where additional safeguards are also in place for data transferred to the United States. Cloudflare will continue to utilize the SCCs mechanism for data transfers, and we have updated our standard customer DPA to incorporate additional safeguards as contractual commitments. For example, we commit that we will pursue legal remedies to contest any U.S. government request for data that we identify as being subject to GDPR, and we commit to notifying our customers of any legal process requesting their information before disclosure of that information, unless legally prohibited. You can view the additional safeguards we have added as contractual commitments in section 7 of our DPA.

Data protection regulations and guidelines are ever-evolving, and we closely monitor the regulatory and legislative landscape. We continually look ahead at emerging guidance to ensure that our customers and partners can continue to enjoy the benefits of Cloudflare across Europe.

For customers who need to ensure that Cloudflare is not transferring any personal data, we offer a set of technical measures known as the Data Localization Suite.

Cloudflare product features designed to support data localisation

Cloudflare is committed to helping our customers keep personal data in the EU. We offer a Data Localization Suite, which gives customers control over where their data is inspected and stored.

Our Data Localization Suite has three elements:

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

Encryption Key Management:

Data privacy is not possible without Internet security, which is provided in large part by effective encryption.

Encryption of data transmitted over a network requires the use of encryption keys, or sets of mathematical values that both the sender and the recipient of an encrypted message know. SSL/TLS, a cryptographic protocol which makes encrypted communication possible, uses a pair of keys — a public key and a private key. Cloudflare customers may choose to use two features to ensure that their private keys do not leave the EU:

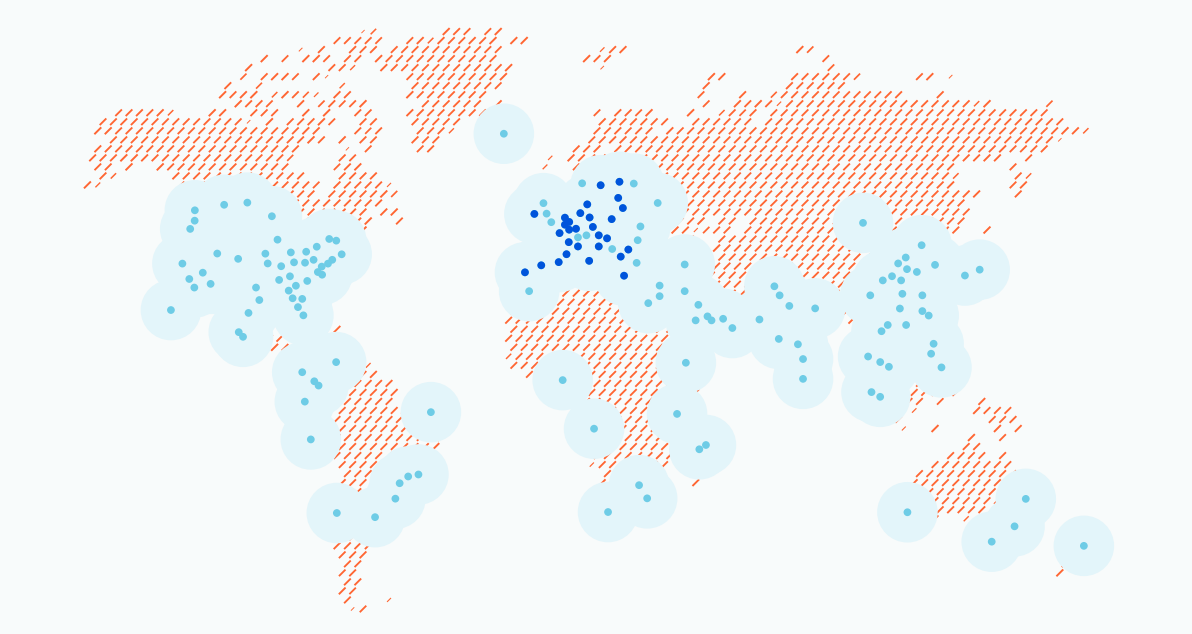
- Keyless SSL allows customers to store and manage their own private keys for use with Cloudflare. Customers can use a variety of systems for their keystore, including hardware security modules ("HSMs"), virtual servers, and hardware running Unix/Linux and Windows housed in environments customers control. 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.
- Geo Key Manager provides customers with granular control over the data centers in which their private keys are stored. For example, a customer can choose for the private keys to only be accessible inside data centers located in the EU. This approach frees customers from the complexity of deploying Keyless SSL and maintaining their own keystore.

Payload Inspection Boundary:

Cloudflare offers the most secure and highest performance network-as-a-service products because we proxy all of your traffic from the edge of our network. As an authorized proxy of your traffic, our services securely inspect your traffic to identify security threats and route it from any location across our global network. Cloudflare is one of the only cloud providers architected as a unified global platform that can also be configured to serve specific regional requirements. This architecture gives Cloudflare customers complete control over where and how traffic is inspected.

Cloudflare's Regional Services lets customers choose where in the Cloudflare network their TLS connections are terminated. For example, a customer could choose to have said connections terminate in the EU, so decryption and inspection of the content of HTTP traffic happens only inside the EU. This restriction applies to all of our edge "application services, including:

- 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



A hypothetical use case would be a Cloudflare customer in Germany enabling Regional Services to limit servicing to the EU. Their end-user clients will connect to the nearest Cloudflare location anywhere in the world, but if that location is outside the EU, the traffic is passed to a Cloudflare EU location before it is inspected. The customer still receives the benefit of our global, low-latency, high-throughput network, which is capable of withstanding even the largest DDoS attacks. However, Regional Services also gives customers local control. Only data centers inside the EU will have the access necessary to apply security policies. This approach allows Cloudflare to select the fastest route to the EU and the closest available point of presence for processing.

Customer Metadata Boundary:

Cloudflare's Customer Metadata Boundary keeps within the EU end-user traffic metadata that can identify a customer.

"Metadata" can be a scary term, but it's a simple concept — it simply means "data about data." In other words, it's a description of activity that happened on our network. Every service on the Internet collects metadata in some form, and it's vital to user safety and network availability.

Cloudflare's network consists of dozens of services: our Firewall, Cache, DNS Resolver, DDoS protection systems, Workers, and more. Each service emits structured log messages, which contain fields like timestamps, URLs, usage of Cloudflare features, and the identifier of the customer's account and zone.

At Cloudflare, we use metadata about the usage of our products for several purposes:

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

Because metadata does not contain the content of customer traffic, it does not contain usernames, passwords, personal information, and other private details of customers' end users. However, service logs may contain end-user IP addresses, which is considered personal data in the EU.

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

Nearly all end user metadata is covered by the Customer Metadata Boundary. This includes all of the end user data for which Cloudflare is a processor, as defined in the Cloudflare Privacy Policy, for the covered services. See here for the most up-to-date list of data types and Cloudflare services covered by the Customer Metadata Boundary.

Shared opportunities and responsibilities

Because we know all European organizations need to integrate privacy and security principles into every aspect of their business, we have prepared this chart to make it easy to understand who is responsible for these commonly requested privacy requirements:

Principle	Responsibility	Responsibility Details
Data protection by design	Shared	Cloudflare is responsible for delivering products and services with privacy in mind. The privacy team provides reviews, assessments, and training to ensure that privacy is instilled in the way we work. Customers are responsible for their usage and configuration of their Cloudflare services, and should periodically review their use and configuration of these services to validate that data protection principles have been considered in the design and implementation.
Subject access request	Shared	Cloudflare provides data subjects with the right of access, correction, and deletion of personal information regardless of their jurisdiction of residence. Data subject requests may be sent to sar@cloudflare.com. If we receive a request from someone who appears to be an end user of one of our customers, we will direct that person to contact our customer directly.

Principle	Responsibility	Responsibility Details
Adequate security	Shared	Cloudflare maintains a security program in accordance with industry standards. The security program includes maintaining formal security policies and procedures, establishing proper logical and physical access controls, implementing technical safeguards in corporate and production environments (including establishing secure configurations, secure transmission and connections, logging, and monitoring), and having adequate encryption technologies for personal data. Customers are responsible for reviewing the security posture of their cloud providers like Cloudflare, and can do so by reviewing our compliance validations and reports. We also encourage our customers to review their Dashboard security settings to ensure they adhere to their security policies and procedures.
Legal basis for processing	Shared	Cloudflare processes data pursuant to the instructions of our customers — the data controllers — and operates as a GDPR-compliant data processor. Customers are responsible for ensuring that they have an appropriate legal basis for processing their end users' data.
Personal data breaches	Shared	Cloudflare will notify customers as soon as we become aware of any breach of security leading to the loss, unauthorised disclosure of, or access to, personal data processed by Cloudflare or its sub-processors. Cloudflare is also responsible for providing our customers with reasonable cooperation and assistance in light of the beach, including providing customers with reasonable information in Cloudflare's possession concerning the circumstances of the breach and the personal data impacted. Customers are responsible for complying with regulatory or contractual requirements to notify their end users and/or government authorities of any personal data breach.

A global cloud network built on customer trust

Cloudflare's first priority is to earn and maintain customer trust. We understand that transparency into Cloudflare's privacy commitments — and into our approach for building data locality and privacy safeguards into our network and products — helps customers meet their own obligations. We also understand that Cloudflare's industry certifications and well-designed contracting mechanisms help us create a strong relationship of trust with our European customers.

Cloudflare's privacy and security teams are here to partner with you to address the most stringent requirements you may face in your country, region, or industry. Our knowledgeable Account Executives, Customer Success Managers, and Sales Engineers partner regularly with our privacy and security compliance teams to help our customers configure the Cloudflare products they use to meet their specific compliance obligations. If you would like a demonstration or specialized session on configuration of your services to meet your unique obligations, contact us today. Please email us at privacyquestions@cloudflare.com or security@cloudflare.com.