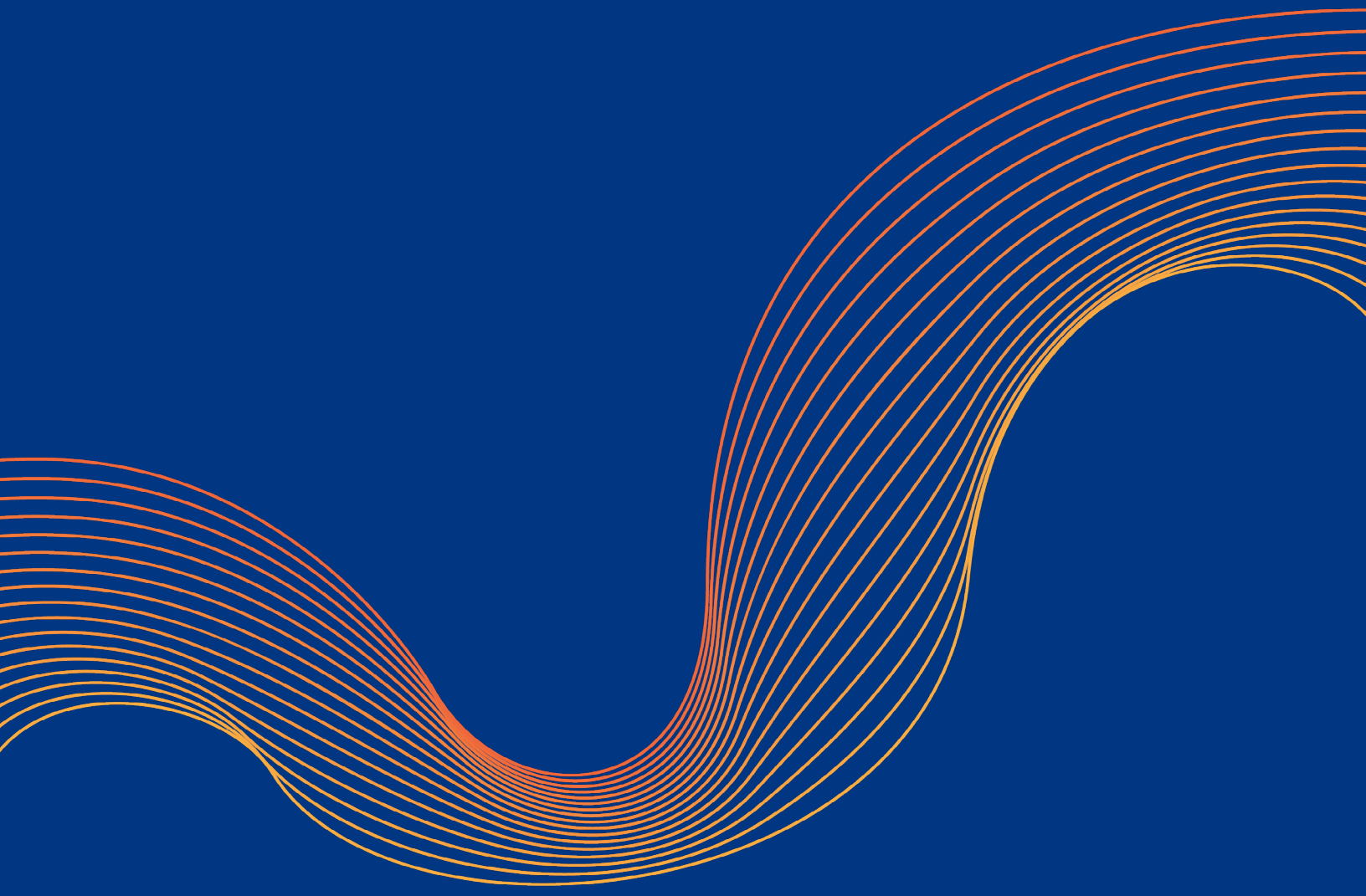
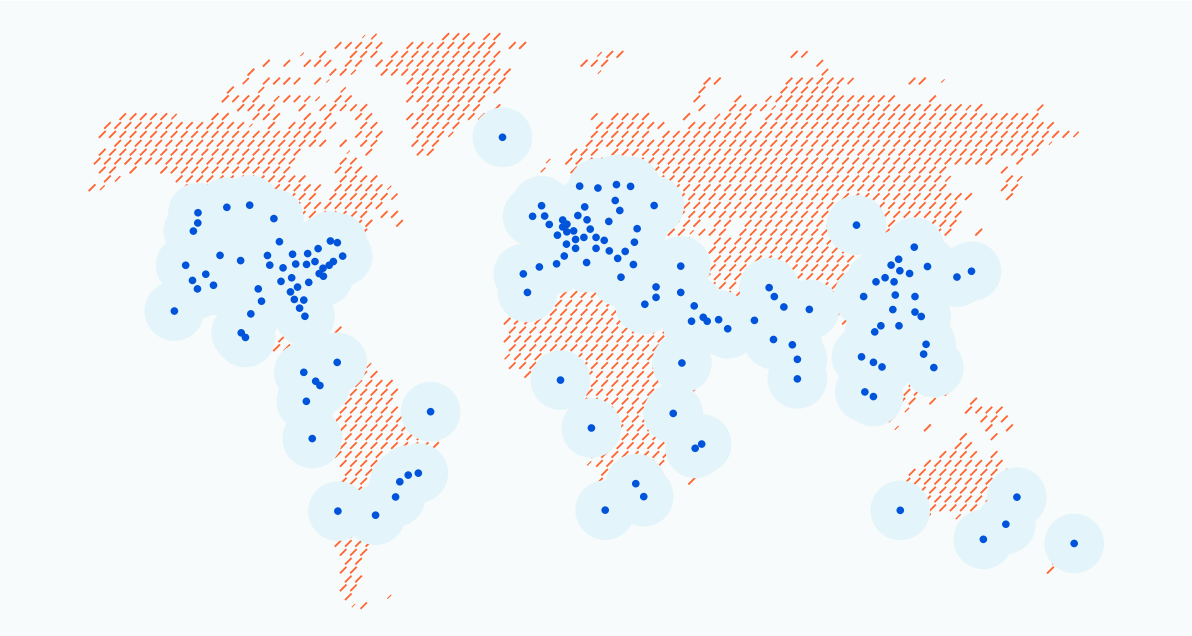
WHITEPAPER

CLOUDFLARE

How Cloudflare Helps Address Data Locality and Privacy Obligations in Europe



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



Cloudflare's unique global cloud network has more than 200 physical points of presence across more than 100 countries. Cloudflare provides you with tools to manage how your sensitive data is routed around these data centers so that you can customize your traffic to meet your security, privacy, and performance needs.

Cloudflare and customer trust

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, 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 across different locations around the world. Finally, we earn customer trust by securing and maintaining industry-defined certifications (e.g. SSAE 18 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, more than 25 million global Internet properties use Cloudflare. This list includes many of Europe's largest and fastest-growing companies, including Eurovision, L'Oreal, AO.com, AllSaints, and many more well-known brands. It also includes a growing list of Europe's important institutions, including INSEAD, Börse Stuttgart, IATA, and Great Rail Journeys. As companies and organizations of all sizes rely more and more on the Internet as a critical platform to serve their customers, users, and stakeholders, they're rapidly adopting secure and reliable cloud networks like Cloudflare to help protect their Internet-facing applications, infrastructure, and people from threats of all kinds.

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.

Cloudflare's unique corporate commitment to privacy

Cloudflare was built to help you and your customers be more secure on the Internet. Our network and all of our products are built with data protection in mind. We are a privacy-first company; 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, and thus default against the collection and retention of personal data we process on your behalf.

As a data processor and service provider, Cloudflare processes end users' log data on behalf of our customers when their end users access our services pursuant to our customers' authorization. This log data processed 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. Our Privacy Policy describes the information we collect and how we use collected information. In addition, in our role as a data controller, Cloudflare collects and stores server and network activity data and logs in the course of operating the Service and makes observations and analysis of traffic data (we call this data "Operational Metrics"). Examples of Operational Metrics include service uptime and service availability metrics, request volumes, error rates, cache rates, and IP threat scores.

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 end users through the least congested and most reliable paths across the Internet. We may also store and analyze network data to detect and identify emerging threat vectors we can immediately use to update how our products protect your Internet properties. Finally, we may aggregate network data from significantly large segments of our customers (but never from individually identifiable users or customers) to help the Internet community understand insights, threats, and trends across the Internet (see Cloudflare Radar). Ultimately, the network data we collect and store is only used to improve our network and our products for our customers, or to share aggregate Internet trends with the broader Internet community.

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 product features designed to support data protection

Our European customers often use the following features to configure their implementation of Cloudflare in order help meet their legal obligations around how data must be handled:

Dashboard & Portal Security:
The Cloudflare Dashboard provides an easy-to-use user interface for customers to configure and manage all of the products they use that run on the Cloudflare network. Customers log in to the Cloudflare Dashboard through Cloudflare's secure web portals. To help customers ensure secure and authorized access to customer Cloudflare accounts and data, we have built standard security features into our portals and Dashboard. We have observed that many companies and organizations struggle to secure access to all of their different security devices, products, and services. In contrast, Cloudflare's products are built on a single, unified and secure platform, so Cloudflare customers benefit from consistent and highly secure account access for all of their security, performance, and reliability products.

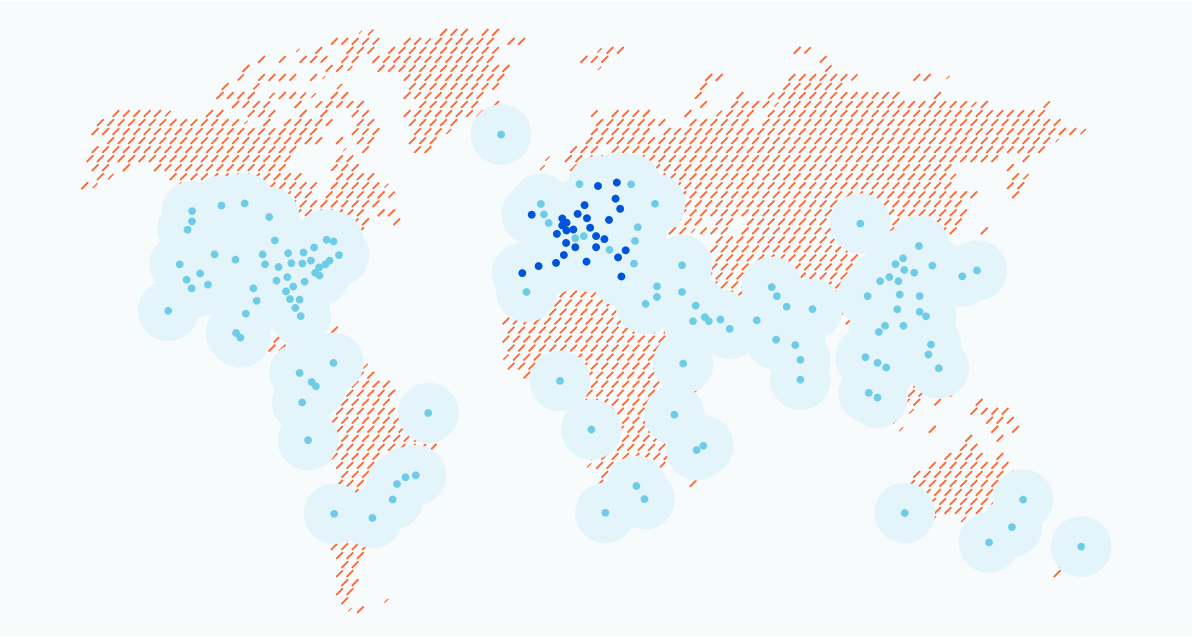
- **Two-factor authentication** (2FA) improves account security by requiring a second piece of information to validate user identity when logging in. Cloudflare 2FA supports hardware tokens and TOTP mobile apps.
- **Single Sign-On** features (when enabled) allows customers to use an on-premise or cloud-hosted identity provider for access control. See the full list of supported providers here.
- **Audit logs** summarize the history of access and changes made to a customer's Cloudflare configuration. Audit logs include account level actions like login and logout, as well as setting changes to DNS, Crypto, Firewall, Speed, Caching, Page Rules, Network, and Traffic features, etc. Audit Logs are available on all plan types and are captured for both individual users and for multi-user organizations.

Encryption:
Encryption is a way of scrambling data so that only authorized parties can understand the information. Data can be encrypted "at rest" when it is stored or "in transit" while it is being transmitted somewhere else. Encryption of data transmitted over a network requires the use of an encryption key: a set of mathematical values that both the sender and the recipient of an encrypted message know.

Encryption prevents unauthorized parties -- whether they are attackers, ad networks, Internet service providers, or hostile foreign actors -- from intercepting and reading sensitive data. Encrypted communications enable the communicating parties to exchange sensitive data without leaking it. Encryption also helps prevent malicious behavior such as on-path attacks. Many industry and government regulations require companies that handle user data to keep that data encrypted. Examples of regulatory and compliance standards that require encryption include HIPAA, PCI-DSS, and the GDPR.

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

Regional Services gives organizations control over where their traffic is inspected. With Regional Services enabled, content traffic is ingested on Cloudflare's global Anycast network at the location closest to the client. Instead of being inspected at that Point of Presence (PoP), this traffic is securely transmitted to Cloudflare PoPs inside the region(s) selected by the customer, where it is then serviced. If Geo Key Manager is also applied, the customer's TLS keys are only stored and used to handle content traffic inside those regions. Regional Services helps customers who want to maintain local control over their traffic while retaining the security benefits of a global network.



For example, a Cloudflare customer in Germany could enable 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.

In addition to specifying where traffic is inspected, Cloudflare helps companies protect users and data by using industry-leading encryption techniques and technologies. Geo Key Manager and Keyless SSL give customers full control over where keys are stored and which PoPs have access to those keys.

Keyless SSL allows a customer to store and manage their own SSL 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 that is housed in environments customers control. Keyless SSL employs several methods to create a secure connection for the key transmission from customer to Cloudflare, and provides session persistence that typically accelerates overall SSL transaction speed.

Geo Key Manager provides customers with granular control over where their keys are stored. For example, a customer can choose for the private keys to only be accessible inside PoPs located in the EU.

With Cloudflare, customers have extensive control over not only where private keys are stored, but also where traffic is actually inspected for security threats. If a customer chooses, only PoPs inside the EU member states will be able to inspect traffic.

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 is compliant with ISO 27001/27002, Payment Card Industry Data Security Standards (PCI DSS), and SSAE 18 SOC 2 Type II. We have signed business associate agreements and are able to support businesses subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). 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, Europe's watershed General Data Protection Regulation (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
- Cloudlfare give 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 our GDPR FAQ here: cloudflare.com/gdpr/introduction.

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. Strong examples are privacy-focused audits, like one we conducted earlier this year 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.

Cloudflare's data transfer mechanisms

The types of personal data Cloudflare processes on behalf of a customer depend on which Cloudflare services are implemented. The vast majority of data that transits Cloudflare's network stays on Cloudflare's edge servers, while log data about this activity may be processed on behalf of our customers in our core data center in the United States — even when customers enable Regional Services.

Some of this log data will include information about the visitors and authorized users of our customer's domains, networks, websites, application programming interfaces ("APIs"), or applications. This metadata contains extremely limited personal data, most often in the form of IP addresses. We process this type of information on behalf of our customers in our core data center in the U.S. for a limited period of time.

As some limited personal data is transferred to the United States, we've made it easy for businesses to maintain a valid data transfer mechanism when using Cloudflare services. Our standard Data Processing Agreement (DPA) is incorporated into our Enterprise Service Agreement, and the DPA incorporates the EU Standard Contractual Clauses (SCCs) 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.

On July 16, 2020, the Court of Justice of the European Union ("CJEU") issued a decision invalidating the EU-US Privacy Shield paradigm in the "Schrems II '' case. As a result, some of our customers who process the data of EU residents have asked us what this decision means for the legality of transferring data Cloudflare processes on their behalf to the United States.
First, the invalidation of the Privacy Shield does not change the strong data privacy protections Cloudflare has in place for the personal data that we process on behalf of our customers, and we will continue to follow the data protection principles we committed to when we certified under the Privacy Shield.

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.

Shared Opportunities and Responsibilities

Because we know all European organizations need to integrate privacy and security principles into each phase of their business, we have prepared this chart to make it easy for you 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 demo 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.

LEARN MORE

1. **Understanding Cloudflare Log Services**
2. **Managing and Analyzing Logs**
3. **Log FAQs**
4. **Contact us** to enable Regional Services