Cloudflare's commitment to GDPR compliance

Last updated: February 1, 2022

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.

Even before Europe's watershed General Data Protection Regulation (GDPR) went into effect in 2018, Cloudflare was focused on how we could improve privacy globally. We've built products to expand and improve privacy online, and we minimize our collection of personal data and only use personal data for the purpose for which it was collected. Since our founding, we have committed that we would keep personal information private, so we have never sold or rented our users' personal information to anyone.

On a practical level, GDPR was a codification of many of the steps we were already taking: only collect the personal data you need to provide the service you're offering; don't sell personal information; give people the ability to access, correct, or delete their personal information; and, consistent with our role as a data processor, give our 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).

We have compiled on this page responses to questions we frequently receive about how we process data on behalf of our customers in a way that complies with the GDPR. As data protection is an ever-evolving environment, we continue to monitor ongoing developments globally and will update this page as appropriate.

Information about the personal data Cloudflare collects, how we use and disclose that information, data subject rights (including how to contact Cloudflare to exercise those rights), and international data transfers can be found in our Privacy Policy.

Contact Our Team

+1 (888) 99 FLARE

About

- Terms of Service
- Privacy Policy
- Sub-Processors
- Data Processing Addendum for Customers
- EU Standard Contractual Clauses
- UK Standard Contractual Clauses

FAQs

1. What personal data does Cloudflare process for its customers and where?

Cloudflare is a security, performance, and reliability company headquartered in the United States (US) that delivers a broad range of network services to businesses of all sizes and in all geographies. We help make them more secure, enhance the performance of their business-critical applications, and eliminate the cost and complexity of managing individual network hardware. Cloudflare's Anycast network – which is powered by more than 200 Edge servers around the world, as described here – serves as the foundation on which we can rapidly develop and deploy our products for our customers.

Cloudflare does not have access to or have any control of the data its customers choose to transmit, route, switch, and cache through the Cloudflare Anycast Network. In a limited number of cases, Cloudflare products can be used for storage of content. Regardless of what Cloudflare services they use, however, our customers are fully responsible for their own compliance with applicable law and their independent contractual arrangements in connection with the data they choose to transmit, route, switch, cache, or store through the Cloudflare Anycast Network.

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 metadata about this

activity is processed on behalf of our customers in our main data center in the United States.

Cloudflare maintains log data about events on our network. Some of this log data will include information about visitors to and/or authorized users of a customer's domains, networks, websites, application programming interfaces ("APIs"), or application, including the Cloudflare product Cloudflare Zero Trust as may be applicable. 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 main data center in the U.S. for a limited period of time.

---

2. What specific technical and organizational security measures does Cloudflare provide for personal data?

Cloudflare views security as a critical element of ensuring data privacy. Since Cloudflare launched in 2010, we've released a number of state-of-the-art, privacy-enhancing technologies, typically ahead of the rest of the industry. Among other things, these tools allow our customers to easily encrypt the content of communications through universal SSL, encrypt the metadata in communications using DNS-over-HTTPS or DNS-over-TLS and encrypted SNI, and control where their SSL keys are held or where their traffic is inspected.

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, and implementing technical safeguards in corporate and production environments, including establishing secure configurations, secure transmission and connections, logging, monitoring, and having adequate encryption technologies for personal data.

We currently maintain the following validations: ISO 27001, SOC 2 Type II, and PCI DSS Level 1 compliance. We also maintain a SOC 3 report. You can learn more about our certifications here.

To view the security measures Cloudflare offers for the protection of personal data, including personal data transferred from the European Union (EU) to the U.S., please see Annex 2 of our standard DPA.

---

3. How does Cloudflare address the requirements of Art. 44 of the GDPR regarding personal data transfers to the U.S.?

The GDPR provides a number of legal mechanisms to ensure that appropriate safeguards, enforceable rights, and effective legal remedies are available for European data subjects whose personal data is transferred from the European Economic Area (EEA) to a third country — a country not covered by the GDPR or deemed to have adequate data protection laws in place.

Those mechanisms include:

- Where the EU Commission has decided that a third country ensures an adequate level of protection after assessing that country's rule of law, respect for human rights and fundamental freedoms, and a number of other factors;
- Where a data controller or processor has put in place binding corporate rules;
- Where a data controller or processor has in place standard data protection clauses adopted by the Commission; or
- Where a data controller or processor has put in place an approved code of conduct or an approved certification mechanism.

Cloudflare relies on the Standard Contractual Clauses (SCCs) as a legal mechanism to transfer personal data from the EEA to the U.S. Previously, Cloudflare also relied on the

and Maximillian Schrems). 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.

---

4. What additional data protection safeguards does Cloudflare provide?

Because we believe earning and maintaining customer trust is essential, Cloudflare has had data protection safeguards in place since well before the Schrems II case. When we issued our very first transparency report in 2014 for legal process received in 2013, we pledged that we would require legal process before providing any government entity with any customer data outside of an emergency and that we would provide our customers with notice of any legal process requesting their customer or billing

information before disclosure of that information unless legally prohibited. We publicly stated that we have never turned over encryption keys to any government, provided any government a feed of content transiting our network, or deployed law enforcement equipment on our network. We also committed that if we were asked to do any of those things, we would "exhaust all legal remedies in order to protect our customers from what we believe are illegal or unconstitutional requests." Since those days early in Cloudflare's history, we have restated those commitments twice a year, and even expanded on them, in our Transparency Reports.

We have also demonstrated our belief in transparency and our commitment to protecting our customers by filing litigation when necessary. In 2013, with the help of the Electronic Frontier Foundation, we legally challenged an administratively issued U.S. national security letter (NSL) to protect our customer's rights because of provisions that allowed the government to restrict us from disclosing information about the NSL to the affected customer. Cloudflare provided no customer information in response to that request, but the non-disclosure provisions remained in effect until a court lifted the restrictions in 2016.

More recently, in a Privacy Day blog post in January 2020, we stated our position that any government requests for personal data that conflicts with the privacy laws of a person's country of residence should be legally challenged. The European Data Protection Board (EDPB) recognized that GDPR might pose such a conflict in an assessment it released last year. Our commitment to compliance with GDPR means that Cloudflare would pursue legal remedies before producing data identified as being subject to GDPR in response to a U.S. government request for data. Consistent with existing U.S. case law and statutory frameworks, Cloudflare may ask U.S. courts to quash a request from U.S. authorities for personal data based on such a conflict of law.

We have updated our standard data processing addendum (DPA) for our customers to now incorporate additional safeguards as contractual commitments. You can view these contractual commitments in section 7 of our DPA.

---

5. Impact of the CJEU Decision on our approach to GDPR compliance

Cloudflare will continue to make the SCCs available to our customers whose data is subject to the GDPR. We are closely following developments in this space as well as around alternative transfer mechanisms.

We understand that in light of the Schrems II case, our customers are seeking additional assurances that data subject to the GDPR and transferred to the U.S. will receive

adequate protection under the GDPR. We discussed those additional safeguards above.

Because the CJEU considered a number of U.S. national security authorities in its analysis in the Schrems II case, we've seen some questions about the application of those authorities to U.S. data processors. Explaining whether, or how, these authorities are relevant to a transfer of data requires some additional explanation of the authorities referenced by the CJEU.

Section 702. Section 702 of the Foreign Intelligence Surveillance Act (FISA) is an authority that allows the U.S. government to request the communications of non-U.S. persons located outside of the United States for foreign intelligence purposes. The U.S. government uses section 702 to collect the content of communications through specifical "selectors", such as email addresses, that are associated with specific foreign intelligence targets. Because the authority is typically used to collect the content of communications, the "electronic communications service providers" asked to comply with section 702 are typically email providers or other providers with access to the content of communications.

As noted in our transparency report, Cloudflare does not generally have access to this type of traditional customer content. In addition, Cloudflare has had a public commitment for many years that we have never provided any government a feed of our customers' content transiting our network and that we would exhaust all legal remedies if we were asked to do so in order to protect our customers from what we believe are illegal or unconstitutional requests.

Executive Order 12333. Executive Order 12333 governs U.S. intelligence agencies' foreign intelligence collection targeting non-U.S. persons outside the United States. Executive Order 12333 does not have provisions to compel the assistance of U.S. companies.

Cloudflare has a longstanding commitment to require legal process before providing any government entity with access to any customer data outside of an emergency. We therefore would not comply with voluntary requests for data under Executive Order 12333. In addition, Cloudflare has been a leader in encouraging additional security for data in transit, for both content and metadata, to prevent personal data from any type of prying eyes. In 2014, for example, we launched Universal SSL, making encryption — something that had been expensive and difficult — free for all Cloudflare customers. The week we launched it, we doubled the size of the encrypted web. Because of an increasing number of laws attempting to target encryption, we have even committed that we have never weakened, compromised, or subverted any of our encryption at the request of a government or other third party.

6. How is Cloudflare responding to the latest EDPB Guidance on Additional Safeguards?

Cloudflare already has in place many of the additional safeguards recommended by the European Data Protection Board (EDPB) in its guidance (Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data adopted on 18 June 2021). Cloudflare has a strong commitment to transparency and accountability regarding processing of personal data as described above, and we have already updated our DPA to make a number of our commitments contractually binding. We also continue to publish our transparency report, which can be viewed here: https://www.cloudflare.com/transparency/. And last but not least, we have in place robust security measures and encryption protocols, which can be viewed in Annex 2 of our DPA.
As always, we are continuing to monitor ongoing developments in this space and will ensure our ongoing compliance with the EU GDPR Articles 44 and 46. During this time, we will continue to follow our commitments under existing DPAs and our commitments under the current SCCs.

---

7. How can Customers who do not have an Enterprise agreement make sure the Standard Contractual Clauses are in place with Cloudflare?

On October 5, 2020, we updated our Self-Serve Subscription Agreement to incorporate our updated standard DPA by reference. And to the extent the personal data we process on behalf of a self-serve customer is governed by the GDPR, then our DPA incorporates the EU standard contractual clauses for this data. So no action is required to ensure that the standard contractual clauses are in place. Our updated DPA also incorporates the additional safeguards described above.

While the DPA is incorporated by reference, we have also made our updated DPA available in the customer dashboard. When you are in your Dashboard, please go to the Configurations tab, and then Preferences.

---

8. How can Enterprise Customers make sure the Standard Contractual Clauses are in place with Cloudflare?

On October 1, 2020, we updated our standard Enterprise Subscription Agreement (ESA) to incorporate our updated standard DPA by reference. Enterprise customers are subject to our standard ESA if they entered into the ESA with Cloudflare on or after August 8,

2019 and do not have a custom agreement. No Action is required for these customers as the updated DPA is incorporated by reference into our ESA, and to the extent the personal data we process on behalf of the customer is governed by the GDPR, then our DPA incorporates the EU standard contractual clauses. Our updated DPA also incorporates the additional safeguards described above. Our updated standard DPA is available here.

Enterprise customers on older versions of our ESA may already have the EU standard contractual clauses in place with Cloudflare. If they do, then no action is needed but they can also agree to our updated DPA available in the customer dashboard, as it includes our additional safeguard language. Customers who were previously relying on Cloudflare's EU-U.S. and Swiss-US Privacy Shield certifications should agree to our updated DPA available in the customer dashboard. When you are in your Dashboard, please go to the Configurations tab, and then Preferences. Please review and accept the DPA there.

Enterprise customers who have a custom agreement with Cloudflare should contact their Customer Success Manager if they have questions about their DPA.

---

9. How is Cloudflare responding to the new Standard Contractual Clauses?

We are carefully reviewing the European Commission's new Standard Contractual Clauses (SCCs) released on 4th June 2021. The new SCCs contain a sunsetting provision of 18 months to allow for implementation, and we will move to implement the new SCCs for our current customers during that timeframe.

---

10. What tools does Cloudflare have for its customers to geographically restrict access to data?

We recognize that some of our customers would prefer that any personal data subject to the GDPR remain in the EU and not be transferred to the U.S. for processing. To that end, we introduced the Cloudflare Data Localization Suite, which 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.

The Data Localisation Suite bundles some existing offerings with some new features:

- ✔ **Regional Services.** Cloudflare has data centers in over 200 cities across 100+

countries. Regional Services together with our Geo Key Manager solution allows Customers to pick the data center locations where TLS keys are stored and TLS termination takes place. Traffic is ingested globally, applying L3/L4 DDoS mitigations, while security, performance, and reliability functions (such as, WAF, CDN, DDoS mitigation, etc.) are serviced at designated Cloudflare data centers only. With Regional Services, some metadata will still be transmitted to our core data center in Portland, Oregon. However, the only Personal Data we collect in these logs are IP addresses.

- **Keyless SSL.** 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.

- **Geo key Manager.** Cloudflare has a truly international customer base and we've learned that customers around the world have different regulatory and statutory requirements, and different risk profiles, concerning the placement of their private keys. With that philosophy in mind, we set out to design a very flexible system for deciding where keys can be kept. Geo Key Manager lets customers limit the exposure of their private keys to certain locations. It's similar to Keyless SSL, but instead of having to run a key server inside your infrastructure, Cloudflare hosts key servers in the locations of your choosing.

- **Edge Log Delivery.** Customers can send logs directly from the edge to their partner of choice—for example, an Azure storage bucket in their preferred region, or an instance of Splunk that runs in an on-premise data center. With this option, customers can still get their complete logs in their preferred region, without these logs first flowing through either of our US or EU core data centers.

- **Jurisdiction Restrictions for Workers Durable Objects.** Durable Objects are a serverless storage and coordination technology that let developers manage state without infrastructure overhead. Jurisdiction Restrictions ensure processing and storage of that data complies with local regulations - while still avoiding any infrastructure configuration by developers. This feature helps development teams to easily build their own compliant, global applications.

---

11. Are there any enforceable rights and effective remedies available to EU data subjects in the U.S. where data is processed by Cloudflare or Cloudflare's sub-processors?

As outlined in our Transparency Report, Cloudflare requires valid legal process before providing the personal information of our customers to government entities or civil litigants, unless there is an emergency. We do not provide our customers' personal information to government officials in response to requests that do not include legal process.

To ensure that our customers have the opportunity to enforce their rights, it is Cloudflare's policy to notify our customers of a subpoena or other legal process requesting their information before disclosure of that information, whether the legal process comes from the government or private parties involved in civil litigation, unless legally prohibited. Specifically, our DPA commits that unless legally prohibited, we will notify Customers if we are able to identify that third-party legal process requesting personal data we process on behalf of that Customer raises a conflict of law — such as where the personal data is governed by the GDPR. Customers notified of a pending legal request for their personal data can seek to intervene to prevent the disclosure of personal data.

In addition, U.S. law provided mechanisms for companies to challenge orders that pose potential conflicts of law, such as a legal request for data subject to GDPR. The Clarifying Lawful Overseas Use of Data (CLOUD) Act, for example, provides mechanisms for a provider to petition a court to quash or modify a legal request that poses such a conflict of law. That process also allows a provider to disclose the existence of the request to a foreign government whose citizen is affected, if that government has signed a CLOUD Act agreement with the United States. Cloudflare has committed to legally challenge any orders that pose such a conflict of law. To date, we have received no orders that we have identified as posing such a conflict.

---

12. What has Cloudflare done to prepare for handling EU personal data prior to Brexit?

We have been paying close attention to the data protection discussions surrounding Brexit and the UK leaving the European Union effective from 1 January 2021, and we have taken steps to ensure we are prepared for the UK adoption of the GDPR into local legislation. Cloudflare will continue to utilize the SCCs mechanism, which are included in our standard DPA to transfer personal data outside the UK and EEA. Please see our instructions above for ensuring you have the appropriate DPA in place. We are continuing to monitor ongoing developments in this space and will ensure our ongoing compliance with UK and global data protection regulations.
