WHITEPAPER

CLOUDFLARE

Cloudflare-Lösung für Datenschutz und Datenlokalisierung in Europa

+49 89 2555 2276 | enterprise@cloudflare.com | www.cloudflare.com/de-de/

KURZFASSUNG

- Cloudflare wurde gegründet, um das Internet für Sie und Ihre Endanwender sicherer zu machen. Datenschutz steht bei uns an erster Stelle und wurde bei der Entwicklung unseres Netzwerks und unserer Produkte von vornherein berücksichtigt.
- Cloudflare setzt ein breites Spektrum an juristischen und vertraglichen Schutzmaßnahmen ein, die mit der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union konform sind.
- Wir bieten eine Reihe von Produktfunktionen und technischen Schutzlösungen für Cloudflare-Kunden an, die nicht möchten, dass ihre Daten Europa verlassen.

Das einzigartige cloudbasierte Netzwerk von Cloudflare umfasst Rechenzentren an mehr als 250 Standorten in über 100 Ländern. Mit den Tools von Cloudflare können Sie festlegen, wie Ihre Daten durch diese Rechenzentren geleitet werden. Sie können selbst bestimmen, wo Ihr Traffic geprüft wird, um Ihren Anforderungen an Sicherheit, Datenschutz und Performance gerecht zu werden.

Über Cloudflare

Cloudflare hat es sich zur Aufgabe gemacht, ein besseres Internet zu schaffen. Unsere globale Cloud-Plattform bietet eine breite Palette von Netzwerkdiensten für Privatpersonen und Unternehmen jeder Größe auf der ganzen Welt. Das Netzwerk und das wachsende Produktportfolio von Cloudflare verbessern die Sicherheit, den Datenschutz, die Performance und die Zuverlässigkeit von allem, was mit dem Internet verbunden ist. Neben der Betreuung unserer Kunden hat es sich Cloudflare auch zur Aufgabe gemacht, das Internet selbst besser zu machen – immer online, schnell, sicher, datenschutzfreundlich und für jeden verfügbar.

Das Netzwerk, die Entwickler-Community und die Geschäftstätigkeit von Cloudflare beruhen letztlich alle auf dem Vertrauen der Kunden. Wir sind bestrebt, das Vertrauen unserer Kunden zu gewinnen und zu bewahren, indem wir uns klar zum Datenschutz bekennen und transparent machen, wie wir die Daten unserer Kunden und Endnutzer in unseren Systemen verwalten. Wir schaffen auch Vertrauen, indem wir Produkte entwickeln und einsetzen, die (i) zur Verbesserung der Sicherheit unserer Systeme beitragen, (ii) Daten im Ruhezustand oder bei der Übertragung verschlüsseln und (iii) unseren Kunden die Möglichkeit geben, zu bestimmen, wie der Datenverkehr an verschiedenen Standorten auf der ganzen Welt geprüft wird. Schließlich gewinnen wir das Vertrauen unserer Kunden, indem wir branchenübliche Zertifizierungen erlangen und beibehalten (z. B. ISO 27001 und 27701, SSAE 18 und SOC 2 Typ II) und Vertragsmechanismen (z. B. Datenverarbeitungsverträge) bereitstellen, die unser Modell der gemeinsamen Verantwortung mit unseren Kunden bei der Gewährleistung des Datenschutzes vermitteln.

Cloudflare in Europa

Aktuell wird Cloudflare für Millionen Websites und Internetanwendungen weltweit genutzt. Darunter sind viele der größten und am schnellsten wachsenden Unternehmen Europas, etwa Eurovision, L'Oreal, AO.com, C&A, AllSaints und zahlreiche weitere bekannte Marken. Dazu zählt

aber auch eine immer länger werdende Liste wichtiger europäischer Institutionen wie INSEAD, die Börse Stuttgart, IATA und Telefonica. Unternehmen und Organisationen unterschiedlichster Größe bauen verstärkt auf das Internet als kritische Plattform zur Bedienung ihrer Kunden, Nutzer und Interessengruppen. Daher setzen sie zunehmend auf sichere und zuverlässige cloudbasierte Netzwerke wie Cloudflare, um ihre Anwendungen, Infrastruktur und Beschäftigten im Web vor Bedrohungen jeder Art zu schützen.

Wir sind uns bewusst, dass Datenschutz in Europa einzigartige Herausforderungen mit sich bringt. Einige davon ergeben sich aus der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union und der Entscheidung des Gerichtshofs der Europäischen Union (EuGH) in der Sache „Schrems II" (Rechtssache C-311/18, *Data Protection Commissioner gegen Facebook Ireland und Maximillian Schrems*). Letztere führte zu weiteren Anforderungen für Unternehmen, die personenbezogene Daten in Länder außerhalb der EU übermitteln. Darüber hinaus verlangen einige stark regulierte Branchen, dass bestimmte Arten personenbezogener Daten die EU nicht verlassen.

Die Internetplattform von Cloudflare ist so aufgebaut, dass sie die am stärksten auf Datenschutz ausgerichteten und regulierten Branchen Europas unterstützt – darunter die Finanzdienstleistungssparte, den öffentlichen Sektor, die Energiebranche, Versorgungsunternehmen, den Einzelhandel, den Bereich Glücksspiel und das Gesundheitswesen. Bei Cloudflare entwickeln wir unsere Produkte so, dass sie den höchsten Sicherheits- und Datenschutzstandards entsprechen. Wir arbeiten zudem eng mit jedem unserer europäischen Kunden zusammen, um sie bei der Erfüllung der Datenschutzverpflichtungen ihres spezifischen Standorts und Branchensegments zu unterstützen.

Wir erreichen dies durch eine Vielzahl von Maßnahmen, darunter:

- das übergreifende unternehmensweite Engagement für den Datenschutz
- die Beibehaltung globaler und europäischer Sicherheitszertifizierungen
- die Aufrechterhaltung DSGVO-konformer Datenübertragungsmechanismen
- das Angebot von Produktfunktionen, die eine Datenlokalisierung unterstützen

In diesem Whitepaper werden diese Elemente im Detail erläutert.

Das einzigartige unternehmensweite Engagement von Cloudflare in Sachen Datenschutz

Cloudflare wurde geschaffen, um Ihnen und Ihren Kunden zu mehr Sicherheit im Internet zu verhelfen. Wir sind ein Unternehmen, bei dem Datenschutz an erster Stelle steht, und unser Netzwerk sowie alle unsere Produkte wurden unter Berücksichtigung des Datenschutzes entwickelt. In unserer Datenschutzrichtlinie verpflichten wir uns, personenbezogene Daten, die wir in Ihrem Auftrag verarbeiten, nicht zu verkaufen oder für andere Zwecke zu verwenden als für die Erbringung unserer Dienstleistungen für Sie. In unserer gesamten Geschichte haben wir dieses Versprechen nie gebrochen. Tatsächlich haben wir unsere Haltung zum Datenschutz schon lange vor Beginn der staatlichen Datenschutzregulierung definiert, die viele andere Technologieunternehmen dazu gezwungen hat, ihre Methoden anzupassen, um den Schutz von Kunden- und Nutzerdaten in angemessener Weise zu berücksichtigen. Wir erzielen keine Werbeeinnahmen und erstellen auch zu keinem Zweck Profile von Endnutzern oder Endnutzerdaten unserer Kunden. Deshalb verzichten wir auf die Erhebung und Speicherung personenbezogener Daten, die wir in Ihrem Auftrag verarbeiten.

Im Folgenden finden Sie einige unserer Datenschutzverpflichtungen, durch die wir uns von vielen anderen Anbietern von Cloud-Diensten unterscheiden:

- Cloudflare verkauft keine personenbezogenen Daten.
- Cloudflare verfolgt die Endnutzer unserer Kunden nicht auf Websites und Internetanwendungen.
- Cloudflare erstellt keine Profile der Endnutzer unserer Kunden zwecks Verkauf von Werbung.
- Cloudflare speichert personenbezogene Daten nur so lange, wie es für die Bereitstellung der Cloudflare-Angebote für unsere Kunden erforderlich ist.

- Cloudflare hat niemals die Kryptoschlüssel unserer Kunden oder einen Feed der unser Netzwerk durchlaufenden Inhalte unserer Kunden an Dritte oder Regierungen weitergegeben. Außerdem haben wir uns bereits vor längerer Zeit dazu verpflichtet, alle Rechtsmittel auszuschöpfen, bevor wir einer solchen Anfrage nachkommen.
- Cloudflare hat öffentlich zugesagt, dass wir alle Rechtsmittel ausschöpfen werden, um jede Anfrage der US-Regierung bezüglich Daten, die unserer Einschätzung nach unter die DSGVO fallen, anzufechten.
- Es gehört zu den Grundsätzen von Cloudflare, unsere Kunden über rechtliche Verfahren zu informieren, in deren Rahmen ihre Daten angefordert werden, bevor diese Daten offengelegt werden – es sei denn, dies ist gesetzlich untersagt.

Internationale und europäische Sicherheitszertifizierungen von Cloudflare

Cloudflare erfüllt die branchenführenden Standards für Sicherheit und Datenschutz und lässt diese Verpflichtungen jährlich von externen Prüfern bestätigen.

Cloudflare wurde nach einem neuen internationalen Datenschutzstandard für den Schutz und die Verwaltung der Verarbeitung personenbezogener Daten zertifiziert: ISO/IEC 27701:2019. Diese Norm ist weniger als zwei Jahre alt und passt das bestehende Konzept des Informationssicherheitsmanagementsystems an die Schaffung eines Datenschutz-Informationsmanagementsystems (Privacy Information Management System – PIMS) an. Es gibt Anforderungen, die sicherstellen, dass dieses Datenschutzmanagementsystem widerstandsfähig ist und kontinuierlich verbessert wird, um die festgelegten Ziele zu erreichen. Die Norm ist so konzipiert, dass die von der Organisationen für die Zertifizierung zu erfüllenden Anforderungen sich sehr eng an den Anforderungen der DSGVO orientieren.

Einfach ausgedrückt, bietet die ISO 27701-Zertifizierung unseren Kunden die Gewissheit, dass wir uns an Datenschutzregeln halten, die von einem Dritten auf die Einhaltung eines auf die DSGVO-abgestimmten, internationalen Branchenstandards überprüft wurden. Somit sind wir dazu verpflichtet, für kontinuierliche Konformität unserer Datenschutzregeln zu sorgen. Neben dem Zusatz zur Datenverarbeitung (Data Processing Addendum – DPA), den wir unseren Kunden im Dashboard zugänglich machen, bietet diese Zertifizierung unseren Kunden in mehrfacher Hinsicht die Zusicherung, dass Cloudflare beim Umgang mit allen von uns verarbeiteten personenbezogenen Daten die Vorgaben der DSGVO einhält.

Darüber hinaus ist Cloudflare ISO 27001/27002-, Payment Card Industry Data Security Standards (PCI DSS)- und SSAE 18 SOC 2 Typ II-konform. Diese Validierungen bieten Unternehmen Sicherheit, die ihre vertraulichsten Daten über unsere Dienste übertragen. Zudem helfen sie ihnen, ihre eigenen Compliance-Verpflichtungen dauerhaft zu erfüllen.

Zusätzlich zu den regelmäßigen Bewertungen durch Dritte anhand von Branchenstandards gilt Cloudflare gemäß der EU-Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie) als „Betreiber wesentlicher Dienste“. Neben der Registrierung gemäß dieser Richtlinie bei den Aufsichtsbehörden ICO (Information Commissioner’s Office) und Ofcom (Office of Communications) in Großbritannien, dem Bundesamt für Sicherheit in der Informationstechnik (BSI) in Deutschland und dem CNCS (Centro Nacional de Cibersegurança) in Portugal wurde Cloudflare auch anhand spezifischer lokaler Anforderungen geprüft, etwa des deutschen BSI-Gesetzes (BSIG). Wir pflegen Beziehungen zu den regionalen europäischen Aufsichtsbehörden und arbeiten eng mit ihnen zusammen, um die Einhaltung der Vorschriften zu gewährleisten. Außerdem bieten wir Einblicke in die Art und Weise, wie wir die Datenschutzanforderungen erfüllen.

In praktischer Hinsicht stellte die DSGVO eine Kodifizierung vieler Schritte dar, die wir bereits unternommen hatten:

- Cloudflare erhebt nur personenbezogenen Daten, die wir zur Bereitstellung der von uns angebotenen Dienstleistung benötigen
- Cloudflare verkauft keine personenbezogenen Daten
- Cloudflare gibt Menschen die Möglichkeit, auf ihre personenbezogen Daten zuzugreifen, sie zu korrigieren oder zu löschen.
- In Übereinstimmung mit unserer Rolle als Auftragsverarbeiter gibt Cloudflare seinen Kunden die Kontrolle über die Informationen, die zum Beispiel in unserem Content Delivery Network (CDN) zwischengespeichert, in der Schlüssel-Werte-Datenbank von Workers gespeichert oder von unserer Web Application Firewall (WAF) erfasst werden

Mehr über unsere Verpflichtung zur Einhaltung der DSGVO erfahren Sie hier:

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

Da uns Datenschutz ein Anliegen ist, nehmen wir nicht nur in den Fällen Audits vor, in denen wir gesetzlich dazu verpflichtet sind oder Zertifizierungen verfügbar sind. Unser Sicherheitsteam führt strenge interne und externe Penetrationstests durch, wir betreiben ein Bug-Bounty-Programm über HackerOne und wir beauftragen externe Prüfer mit der Validierung unserer Datenschutzverpflichtungen. Ein gutes Beispiel dafür sind datenschutzorientierte Audits, wie die von uns durchgeführte Überprüfung zu unseren Verpflichtungen hinsichtlich unseres öffentlichen DNS-Resolvers 1.1.1.1. Wir sind immer offen für zusätzliche Validierungen, die uns Gewissheit über unsere Datenschutzregeln sowie unsere Richtlinien und Methoden zur Verarbeitung und Speicherung personenbezogener Daten aus der EU verschaffen.

Von Cloudflare verarbeitete Daten

Cloudflare verarbeitet die Protokolldaten der Endnutzer unserer Kunden, wenn diese Endnutzer entsprechend der Autorisierung unserer Kunden auf unsere Dienste zugreifen. Diese Protokolldaten können unter anderem IP-Adressen, Informationen zur Systemkonfiguration und andere Informationen über den ein- und ausgehenden Datenverkehr von Websites, Geräten, Anwendungen und/oder Netzwerken unserer Kunden enthalten. Cloudflare erfasst und speichert darüber hinaus Server- und Netzwerk-Aktivitätsdaten sowie Protokolle im Rahmen des Betriebs unserer Produkte. Zudem werden Traffic-Daten von uns überwacht und analysiert. Unsere Datenschutzrichtlinie beschreibt genauer, welche Informationen wir erheben und wie wir diese verwenden.

Daten aus Aktivitäten in unserem Netzwerk werden von uns nur erhoben und gespeichert, um unsere Produkte für Sie, unsere anderen Kunden oder die Internet-Community im Allgemeinen zu verbessern. Wir versuchen nicht, diese Daten in irgendeiner Weise zu monetarisieren, sondern verwenden die Netzwerkdaten ausschließlich zur Erbringung unserer Services und Dienstleistungen. Wir speichern und analysieren vorübergehend Daten zum Netzwerk-Traffic von allen unseren weltweiten Kunden, sodass wir Anfragen auf intelligente Weise über die effizientesten Internetpfade leiten können. Netzwerkdaten werden von uns gespeichert und analysiert, um neue Bedrohungsvektoren aufzuspüren und zu identifizieren. Diese Erkenntnisse können wir dann sofort zur Verbesserung unserer Sicherheitstools nutzen. Schließlich können wir Netzwerkdaten von größeren Kundensegmenten (aber niemals von individuell identifizierbaren Nutzern oder Kunden) bündeln, um der Internet-Community dabei zu helfen, Trends und Bedrohungen im gesamten Web zu verstehen (mehr dazu bei Cloudflare Radar).

Die Datenübertragungsmechanismen von Cloudflare

Für den Fall, dass Cloudflare als Auftragsverarbeiter personenbezogene Daten an Ziele außerhalb der EU übermittelt, tun wir dies im Rahmen unseres Zusatz zur Datenverarbeitung (Data Processing Addendum – DPA), der sowohl in unseren Enterprise-Leistungsvertrag als auch in unseren Self-Serve-Abonnementvertrag integriert ist. Unser DPA enthält die EU-Standardvertragsklauseln (in der aktualisierten Fassung des Jahres 2021) für Daten, die der DSGVO unterliegen. Zusammengenommen gewährleisten die Bestimmungen von Cloudflare ein Schutzniveau für personenbezogene Daten, das dem der DSGVO entspricht. Weitere Informationen über unsere Verpflichtung zur Einhaltung der DSGVO und über unseren DPA finden Sie hier.

Gemäß der Schrems-II-Entscheidung sind in der EU zugelassene Standardvertragsklauseln nach wie vor ein gültiger Übermittlungsmechanismus im Rahmen der DSGVO, wenn zusätzliche Garantien auch für Datenübermittlungen in die Vereinigten Staaten bestehen. Cloudflare wird weiterhin den Standardvertragsklausel-Mechanismus für Datenübertragungen nutzen. Außerdem haben wir unseren Standard-DPA für Kunden aktualisiert, um zusätzliche Sicherheitsvorkehrungen als vertragliche Verpflichtungen aufzunehmen. So verpflichten wir uns beispielsweise, alle Rechtsmittel auszuschöpfen, um jede Datenanfrage der US-Regierung anzufechten, die unserer Einschätzung nach der DSGVO unterliegen. Darüber hinaus verpflichten wir uns auch, unsere Kunden vor der Offenlegung ihrer Daten über jedes rechtliche Verfahren zu informieren, in dessen Rahmen ihre Daten angefordert werden, sofern dies nicht gesetzlich untersagt ist. Die zusätzlichen Schutzmaßnahmen, die wir als vertragliche Verpflichtungen hinzugefügt haben, können Sie in Abschnitt 7 unseres DPA einsehen.

Die Datenschutzbestimmungen und -richtlinien entwickeln sich ständig weiter und wir verfolgen den Wandel der ordnungspolitischen und gesetzlichen Rahmenbedingungen genau. Wir schauen ständig auf neue Richtlinien, um sicherzustellen, dass unsere Kunden und Partner weiterhin die Vorteile von Cloudflare in ganz Europa genießen können.

Kunden, die sicherstellen müssen, dass Cloudflare *keinerlei* personenbezogene Daten überträgt, können dafür die Lösungen unserer Data Localisation Suite nutzen.

Datenlokalisierungsfunktionen von Cloudflare-Produkten

Cloudflare will unseren Kunden dabei helfen, dafür zu sorgen, dass ihre personenbezogenen Daten die EU nicht verlassen. Wir bieten deshalb eine Data Localisation Suite an, die den Kunden die Kontrolle darüber gibt, wo ihre Daten geprüft und gespeichert werden.

Unsere Data Localisation Suite besteht aus drei Elementen:

1. Verwaltung von Kryptoschlüsseln (Geo Key Manager und Keyless SSL)
2. Schwelle für Payload-Überprüfungen (Regional Services)
3. Metadata Boundary für Kunden

Verwaltung von Kryptoschlüsseln:

Datenschutz ist ohne Internetsicherheit nicht möglich, und diese wird zum großen Teil durch wirksame Verschlüsselung gewährleistet.

Die Verschlüsselung von Daten, die über ein Netzwerk übertragen werden, erfordert Kryptoschlüssel bzw. Sätze mathematischer Werte, die sowohl dem Absender als auch dem Empfänger einer verschlüsselten Nachricht bekannt sind. Das Verschlüsselungsprotokoll SSL/TLS, das die verschlüsselte Kommunikation ermöglicht, verwendet ein Schlüsselpaar: einen öffentlichen und einen privaten Schlüssel. Cloudflare-Kunden können zwei Funktionen nutzen, um sicherzustellen, dass ihre privaten Schlüssel die EU nicht verlassen:

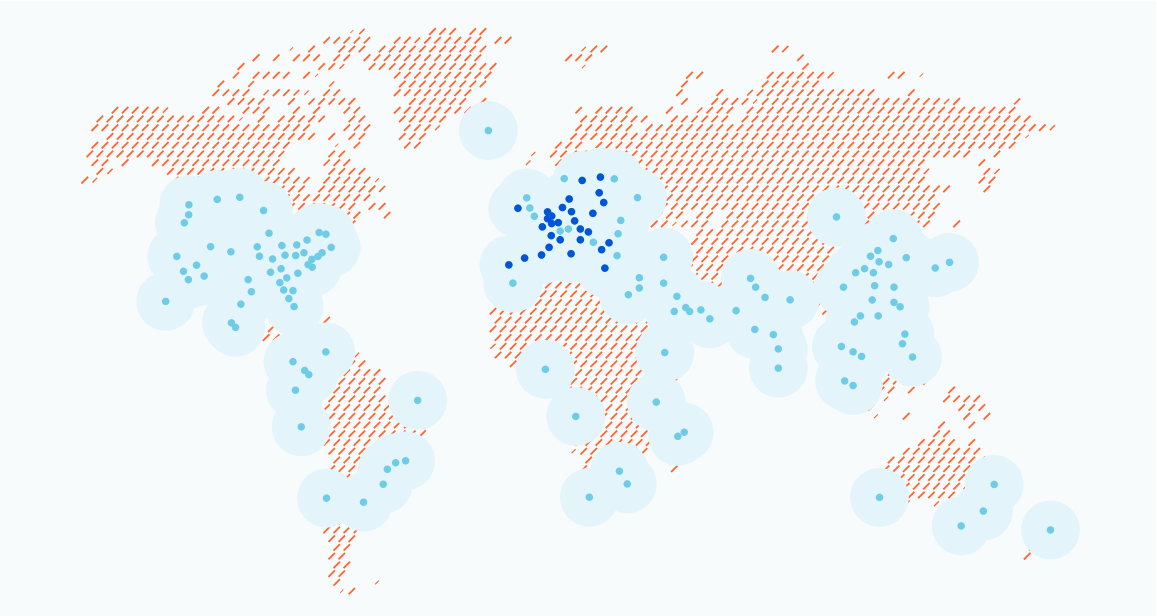
- Keyless SSL erlaubt es Kunden, ihre eigenen privaten Schlüssel für die Verwendung mit Cloudflare zu speichern und zu verwalten. Die Kunden können eine Vielzahl von Systemen für ihren Schlüsselspeicher verwenden, darunter Hardware-Sicherheitsmodule (HSM), virtuelle Server und Hardware, auf der Unix/Linux und Windows laufen und die sich in vom Kunden kontrollierten Umgebungen befindet. Keyless SSL ist nur aus der Sicht von Cloudflare schlüssellos: Cloudflare sieht den privaten Schlüssel des Kunden nie, aber der Kunde verfügt über diesen und nutzt ihn. Der öffentliche Schlüssel wird unterdessen auf Client-Seite weiterhin wie gewohnt verwendet.
- Der Geo Key Manager bietet den Kunden eine präzisere Kontrolle über die Rechenzentren, in denen ihre privaten Schlüssel gespeichert sind. So kann ein Kunde beispielsweise festlegen, dass die privaten Schlüssel nur in Rechenzentren in der EU zugänglich sind. Dieser Ansatz befreit die Kunden von der Komplexität der Bereitstellung von Keyless SSL und der Verwaltung ihres eigenen Schlüsselspeichers.

Schwelle für Payload-Überprüfungen:

Cloudflare bietet die sichersten und leistungsstärksten Network as a Service-Produkte, da wir Ihren gesamten Datenverkehr vom Rand unseres Netzwerks aus weiterleiten. Unsere Dienste sind als Proxy für Ihren Traffic autorisiert, sodass sie ihn auf sichere Weise überprüfen können, um Bedrohungen zu erkennen. Anschließend wird er von jedem Standort aus über unser globales Netzwerk weitergeleitet. Cloudflare ist einer der wenigen Cloud-Anbieter, der als einheitliche globale Plattform konzipiert ist, die auch für spezifische regionale Anforderungen konfiguriert werden kann. Diese Architektur gibt Cloudflare-Kunden die vollständige Kontrolle darüber, wo und wie der Datenverkehr inspiziert wird.

Mit den Regional Services von Cloudflare können Kunden wählen, wo im Cloudflare-Netzwerk ihre TLS-Verbindungen beendet werden. Ein Kunde könnte sich beispielsweise dafür entscheiden, die Verbindungen in der EU enden zu lassen, sodass die Entschlüsselung und Überprüfung des Inhalts des HTTP-Traffics nur innerhalb der EU erfolgt. Diese Einschränkung gilt für alle unsere Edge-Anwendungs-Dienstleistungen, einschließlich:

- Speichern und Abrufen von Inhalten aus dem Cache
- Blockieren bösartiger HTTP-Nutzdaten mit der Web Application Firewall (WAF)
- Erkennen und Blockieren verdächtiger Aktivitäten mit Bot-Management
- Ausführen von Workers-Skripten



Ein hypothetischer Anwendungsfall wäre ein Cloudflare-Kunde in Deutschland, der Regional Services aktiviert, um den Dienst auf die EU zu beschränken. Ihre Endnutzer-Clients stellen eine Verbindung zum nächstgelegenen Cloudflare-Standort in der ganzen Welt her. Liegt dieser Standort jedoch außerhalb der EU, wird der Datenverkehr an einen Cloudflare-Standort in der EU weitergeleitet, bevor er geprüft wird. Der Kunde profitiert weiterhin von der niedrigen Latenz und dem hohen Datendurchsatz unseres globalen Netzwerks, das selbst den größten DDoS-Angriffen standhalten kann. Die Regional Services geben den Kunden aber auch die Möglichkeit der lokalen Kontrolle. Nur Rechenzentren innerhalb der EU haben die notwendigen Zugriffsrechte, um Sicherheitsmaßnahmen anzuwenden. Auf diese Weise kann Cloudflare den schnellsten Weg in die EU und den nächstgelegenen Standort für die Verarbeitung auswählen.

Schwelle für Kunden-Metadaten (Customer Metadata Boundary):

Dieser Cloudflare-Dienst stellt sicher, dass Metadaten des Endnutzer-Traffics, anhand derer ein Kunde identifiziert werden könnte, die EU nicht verlassen.

Der Begriff „Metadaten“ mag auf den ersten Blick abschreckend wirken, bezeichnet aber einfach nur „Daten über Daten“. Anders ausgedrückt handelt es sich um eine Beschreibung von Aktivitäten, die in unserem Netzwerk stattgefunden haben. Jeder Dienst im Internet erfasst in irgendeiner Form Metadaten, die für die Sicherheit der Nutzer und die Verfügbarkeit des Netzwerks unerlässlich sind.

Das Netzwerk von Cloudflare besteht aus Dutzenden von Diensten, darunter unsere Firewall, der Cache, der DNS-Resolver, die DDoS-Abwehrsysteme und Workers. Jeder Dienst gibt strukturierte Protokollnachrichten aus, die Felder wie Zeitstempel, URLs, die Nutzung von Cloudflare-Funktionen sowie die Kennung des Kundenkontos und der Zone enthalten.

Bei Cloudflare verwenden wir Metadaten über die Nutzung unserer Produkte für verschiedene Zwecke:

- Bereitstellung von Analysen über unsere Dashboards und APIs
- Weitergabe von Protokollen an Kunden
- Neutralisierung von Sicherheitsbedrohungen wie Bots oder DDoS-Angriffen
- Verbesserung der Performance unseres Netzwerks
- Aufrechterhaltung der Zuverlässigkeit und Ausfallsicherheit unseres Netzwerks

Da der Inhalt des Kunden-Traffics von den Metadaten nicht abgedeckt ist, umfassen diese auch keine Benutzernamen, Passwörter, personenbezogenen Daten und andere private Informationen der Endnutzer der Kunden. Die Dienstprotokolle können jedoch die IP-Adressen der Endnutzer enthalten, die in der EU unter die Kategorie „personenbezogene Daten“ fallen.

Bei aktivierter Metadata Boundary stellt unsere Edge sicher, dass keine Protokollnachricht, anhand derer ein betreffender Kunde identifiziert werden könnte (die also die Konto-ID dieses Kunden enthält), an ein Ziel außerhalb der EU gesendet wird. Die Daten werden nur an unser zentrales Rechenzentrum in der EU übertragen, nicht jedoch an unser zentrales Rechenzentrum in den Vereinigten Staaten.

Nahezu alle endnutzerbezogenen Metadaten werden durch die Customer Metadata Boundary abgedeckt. Dies umfasst alle Endnutzerdaten, für die Cloudflare als Auftragsverarbeiter fungiert, wie in der Datenschutzrichtlinie von Cloudflare ür die abgedeckten Dienste definiert. Die aktuellste Liste der von der Customer Metadata Boundary umfassten Datentypen und Cloudflare-Dienste finden Sie hier.

Gemeinsame Chancen und Zuständigkeit

Uns ist bewusst, dass alle europäischen Organisationen Datenschutz- und Sicherheitsgrundsätze in jeden Bereich ihrer Geschäftstätigkeit einbeziehen müssen. Deshalb haben wir diese Tabelle erstellt, um deutlich zu machen, wem die Verantwortung für diese gemeinhin geltenden Datenschutzanforderungen jeweils obliegt:

Grundsatz	Zuständigkeit	Einzelheiten zur Zuständigkeit
Von vornherein integrierter Datenschutz	Gemeinsam	Cloudflare ist verantwortlich für die Bereitstellung datenschutzorientierter Produkte und Dienstleistungen. Das Datenschutzteam bietet Überprüfungen, Bewertungen und Schulungen, um sicherzustellen, dass der Datenschutz in unserer Arbeitsweise verankert ist. Die Kunden sind für die Nutzung und Konfiguration ihrer Cloudflare-Dienste verantwortlich und sollten ihre Nutzung und Konfiguration dieser Dienste regelmäßig daraufhin überprüfen, ob bei der Entwicklung und Implementierung Datenschutzgrundsätze berücksichtigt wurden.
Antrag auf Auskunftserteilung	Gemeinsam	Cloudflare bietet betroffenen Personen unabhängig von ihrem Wohnsitzland bezüglich ihrer personenbezogenen Daten das Auskunftsrecht, das Recht auf Berichtigung und das Recht auf Löschung an. Anfragen von betroffenen Personen können an sar@cloudflare.com gerichtet werden. Wenn wir eine Anfrage von jemandem erhalten, der ein Endnutzer eines unserer Kunden zu sein scheint, werden wir diese Person anweisen, sich direkt an unseren Kunden zu wenden.

Grundsatz	Zuständigkeit	Einzelheiten zur Zuständigkeit
Angemessene Sicherheit	Gemeinsam	Cloudflare wendet ein Sicherheitskonzept an, das den Branchenstandards entspricht. Das Sicherheitskonzept umfasst die Aufrechterhaltung formaler Sicherheitsrichtlinien und -verfahren, die Einrichtung angemessener logischer und physischer Zugriffskontrollen, die Implementierung technischer Schutzmaßnahmen in Unternehmens- und Produktionsumgebungen (einschließlich der Einrichtung sicherer Konfigurationen, sicherer Übertragungen und Verbindungen, Protokollierung und Überwachung) und die Bereitstellung angemessener Verschlüsselungstechnologien für personenbezogene Daten. Es liegt in der Verantwortung der Kunden, das Sicherheitsniveau der von ihnen genutzten Cloud-Anbieter (beispielsweise Cloudflare) zu überprüfen. Hierfür können sie Einsicht in unsere Compliance-Validierungen und -Berichte nehmen. Wir empfehlen unseren Kunden außerdem, ihre Dashboard-Sicherheitseinstellungen zu überprüfen, um zu gewährleisten, dass sie ihre Sicherheitsrichtlinien und -verfahren einhalten.
Rechtsgrundlage für die Verarbeitung	Gemeinsam	Cloudflare verarbeitet Daten gemäß den Anweisungen unserer Kunden – den Datenverantwortlichen – und arbeitet als DSGVO-konformer Auftragsverarbeiter. Die Kunden müssen sicherstellen, dass sie über eine angemessene Rechtsgrundlage für die Verarbeitung der Daten ihrer Endnutzer verfügen.
Sicherheitsverletzung bezüglich personenbezogener Daten	Gemeinsam	Sobald wir von einer Sicherheitsverletzung Kenntnis erlangen, die zum Verlust personenbezogener Daten, die von Cloudflare oder unseren Unterauftragsverarbeitern verarbeitet werden, zur unbefugten Offenlegung dieser Daten oder zum Zugriff auf diese Daten führt, informieren wir die betroffenen Kunden. Cloudflare ist auch dafür verantwortlich, unseren Kunden eine angemessene Zusammenarbeit und Unterstützung im Hinblick auf die Sicherheitsverletzung zu bieten. Dies umfasst die Bereitstellung von angemessenen Informationen im Besitz von Cloudflare über die Umstände der Verletzung und die betroffenen personenbezogenen Daten. Es liegt in der Verantwortung der Kunden, die gesetzlichen oder vertraglichen Anforderungen zu erfüllen, um seine Endnutzer und/oder Behörden über jede Verletzung des Schutzes personenbezogener Daten zu informieren.

Ein globales Cloud-Netzwerk, das auf dem Vertrauen der Kunden beruht

Die oberste Priorität von Cloudflare ist es, das Vertrauen der Kunden zu gewinnen und zu bewahren. Uns ist bewusst, dass Transparenz in Bezug auf die Datenschutzverpflichtungen von Cloudflare – und in Bezug auf unseren Ansatz, Datenlokalisierung und Datenschutzgarantien in unser Netzwerk und unsere Produkte zu integrieren – unseren Kunden dabei hilft, ihre eigenen Verpflichtungen zu erfüllen. Wir wissen auch, dass die Branchenzertifizierungen von Cloudflare und die gut durchdachten Vertragsmechanismen uns helfen, ein starkes Vertrauensverhältnis zu unseren europäischen Kunden aufzubauen.

Die Datenschutz- und Sicherheitsteams von Cloudflare arbeiten mit Ihnen zusammen, um die strengsten Anforderungen zu erfüllen, die in Ihrem Land, Ihrer Region oder Ihrer Branche möglicherweise gelten. Unsere sachkundigen Account Executives, Customer Success Manager und Sales Engineers arbeiten regelmäßig mit unseren Datenschutz- und Sicherheits-Compliance-Teams zusammen, um unseren Kunden bei der Konfiguration der von ihnen verwendeten Cloudflare-Produkte zu helfen, damit sie ihre spezifischen Compliance-Verpflichtungen einhalten können. Wenn Sie eine Demonstration oder eine Sondersitzung zur Konfiguration Ihrer Dienste wünschen, um Ihre individuellen Anforderungen zu erfüllen, kontaktieren Sie uns noch heute. Bitte senden Sie uns eine E-Mail an privacyquestions@cloudflare.com oder security@cloudflare.com.