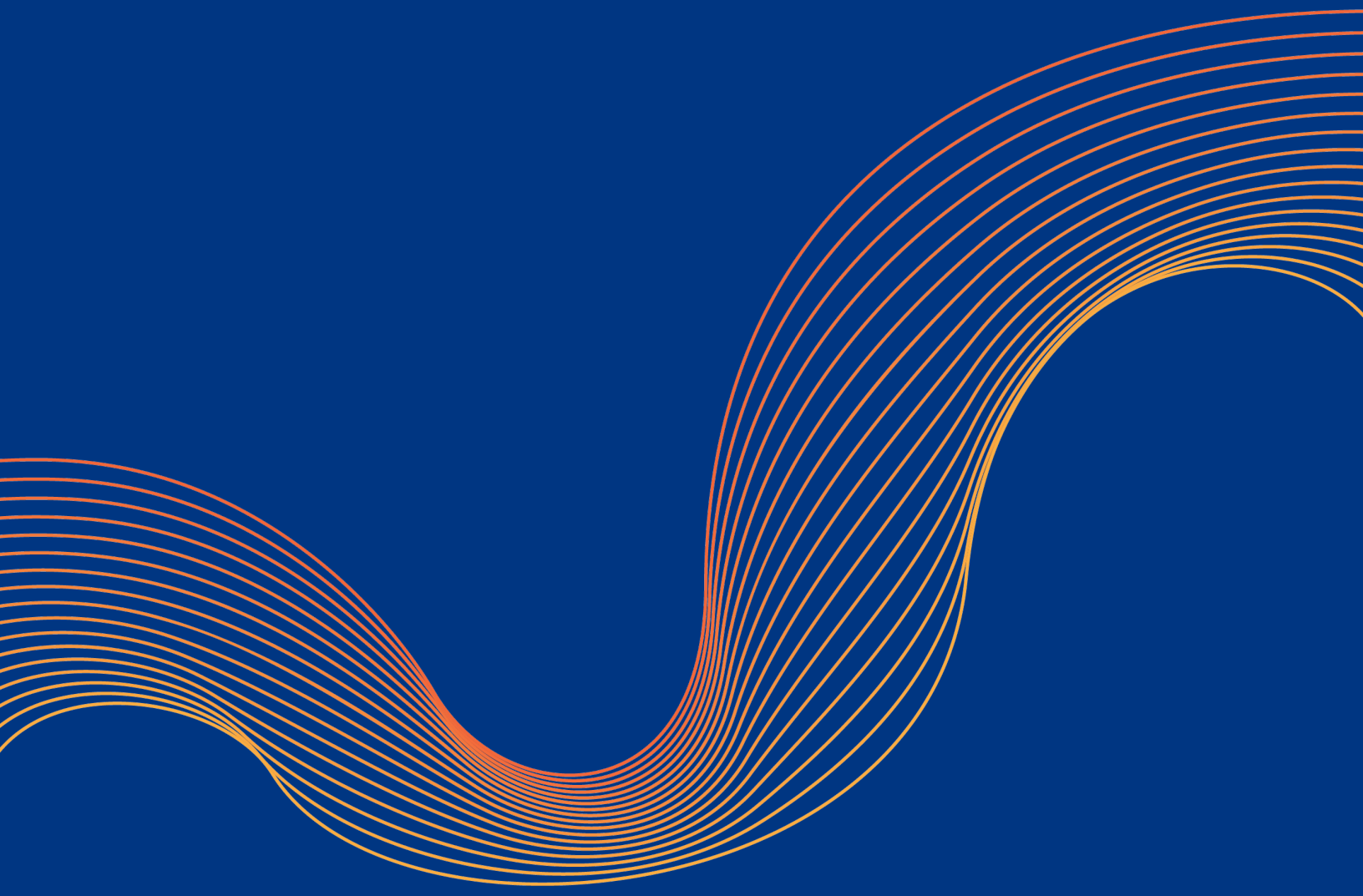
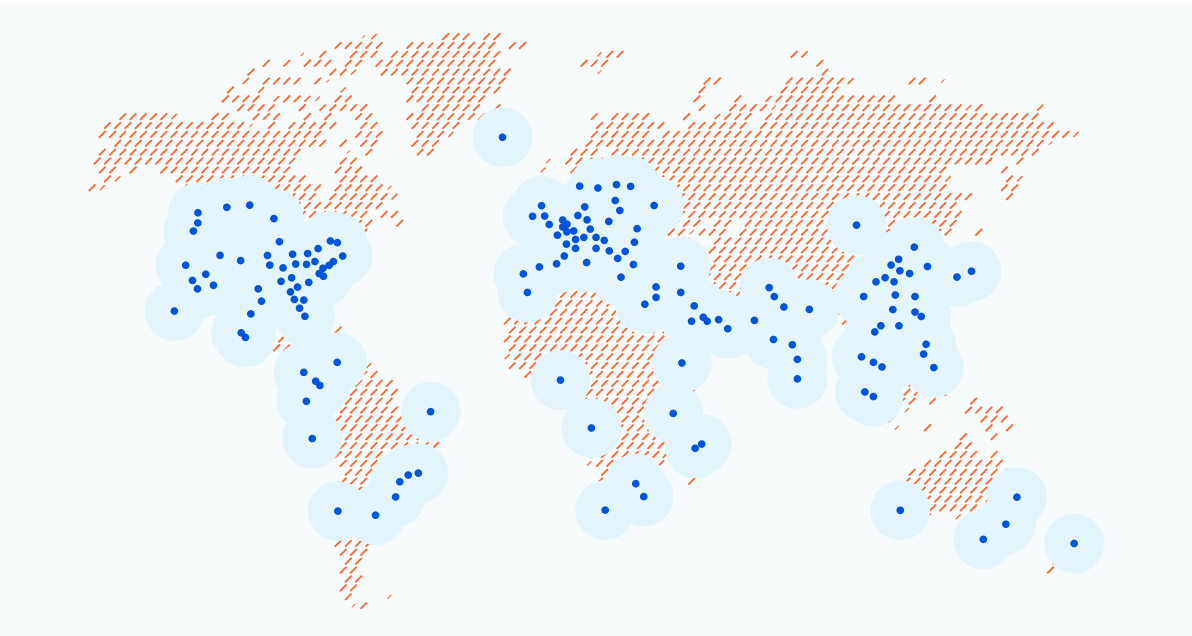
WHITEPAPER

CLOUDFLARE

Wie Cloudflare zur Einhaltung der Datenlokalisierungs- und Datenschutzvorschriften in Europa beiträgt



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



Das einzigartige weltweite Cloud-Netzwerk von Cloudflare verfügt über mehr als 200 physische Points of Presence (Knotenpunkte) in mehr als 100 Ländern. Cloudflare stellt Ihnen Tools zur Verfügung, mit denen Sie festlegen können, welche Rechenzentren Sie für Ihre sensiblen Daten nutzen möchten. Damit können Sie Ihren Traffic individuell auf Ihre Sicherheits-, Datenschutz- und Performance-Anforderungen abstimmen.

Cloudflare und Kundenvertrauen

Cloudflare hat das Ziel, zu einem besseren Internet beizutragen. Wir stellen eine globale Cloud-Plattform bereit, die Privatpersonen und Unternehmen jeder Größe auf der ganzen Welt eine breite Palette von Netzwerkdiensten bietet. Das Netzwerk und das wachsende Produktsortiment von Cloudflare verbessern die Sicherheit, Performance und Zuverlässigkeit jedes Geräts, das mit dem Internet verbunden ist. Neben dem Dienst an unseren Kunden besteht die Aufgabe von Cloudflare zudem darin, dazu beizutragen, das Internet selbst besser zu machen – damit es stets funktionsfähig, schnell, sicher, privat und für jeden verfügbar ist.

Das Netzwerk, die Entwickler-Gemeinde und das Geschäft von Cloudflare beruhen letztlich alle auf dem Vertrauen der Kunden. Um dieses zu gewinnen und zu bewahren, sind wir stets transparent im Hinblick auf unser Engagement für den Datenschutz und den Umgang mit Kunden- und Endnutzerdaten innerhalb unserer Systeme. Wir bauen zudem Vertrauen auf, indem wir Produkte entwickeln und bereitstellen, die (i) zur Verbesserung der Sicherheit unserer Systeme beitragen, (ii) Daten im Ruhezustand oder bei der Übertragung verschlüsseln und (iii) unseren Kunden ermöglichen, zu bestimmen, wie der Traffic an verschiedenen Standorten auf der ganzen Welt geprüft wird. Schließlich gewinnen wir das Vertrauen unserer Kunden, indem wir branchendefinierte Zertifikate (z. B. SSAE 18 SOC 2 Typ II) absichern und aufrechterhalten, und Vertragsmechanismen (z. B. Vereinbarungen zur Datenverarbeitung) bereitstellen, die unser Modell der gemeinsamen Verantwortung gegenüber unseren Kunden bei der Gewährleistung des Datenschutzes vermitteln.

Cloudflare in Europa

Heute nutzen weltweit mehr als 25 Millionen Internetwebsites Cloudflare. Dazu zählen viele der größten und am schnellsten wachsenden Unternehmen Europas, darunter Eurovision, L'Oreal, AO.com, AllSaints und zahlreiche weitere bekannte Marken. Hinzu kommt eine wachsende Zahl wichtiger europäischer Institutionen, etwa INSEAD, Börse Stuttgart, IATA und Great Rail Journeys. Da sich Unternehmen und Organisationen unterschiedlichster Größe immer mehr auf das Internet als kritische Plattform verlassen, um ihren Kunden, Anwendern und Interessenvertretern ihre Produkte und Dienste zur Verfügung zu stellen, führen sie schnell sichere und zuverlässige Cloud-Netzwerke wie Cloudflare ein, um ihre mit dem Internet verbundenen Anwendungen, Infrastrukturen und Mitarbeiter vor Bedrohungen aller Art zu schützen.

Die Internetplattform von Cloudflare wurde entwickelt, um die datenschutzbewusstesten und am stärksten regulierten Branchen Europas zu unterstützen, darunter die Finanzdienstleistungsindustrie, der öffentliche Sektor, die Energiesparte, Versorgungsunternehmen, der Einzelhandel, der Bereich Glücksspiele und das Gesundheitswesen. Bei Cloudflare bauen wir unsere Produkte so, dass sie den höchsten Sicherheits- und Datenschutzstandards entsprechen. Wir arbeiten eng mit jedem unserer europäischen Kunden zusammen, um diese bei der Erfüllung der mit ihrem konkreten Standort und Branchensegment verbundenen Datenschutzverpflichtungen zu unterstützen.

Das besondere Engagement von Cloudflare für den Datenschutz

Cloudflare wurde entwickelt, um Ihnen und Ihren Kunden mehr Sicherheit im Internet zu bieten. Unser Netzwerk und alle unsere Produkte wurden mit Blick auf den Datenschutz entwickelt. Wir sind ein Unternehmen, bei dem Datenschutz an erster Stelle steht. In unserer Datenschutzrichtlinie verpflichten wir uns, dass wir personenbezogene Daten, die wir in Ihrem Auftrag verarbeiten, weder verkaufen noch für andere Zwecke verwenden, außer Ihnen unsere Dienste bereitzustellen. In unserer gesamten Unternehmensgeschichte haben wir dieses Versprechen nie gebrochen. Tatsächlich stand unsere Haltung zum Datenschutz bereits fest, lange bevor die Regierungen begannen, den Datenschutz auf eine Weise zu regulieren, die viele andere Technologieunternehmen dazu zwang, ihre Verfahrensweisen anzupassen, um dem Schutz von Kunden- und Benutzerdaten angemessene Priorität einzuräumen. Wir erzielen keine Werbeeinnahmen und lehnen die Erhebung und Speicherung von personenbezogenen Daten ab, die wir in Ihrem Namen verarbeiten.

Als Auftragsverarbeiter und Service-Provider verarbeitet die Firma Cloudflare die Protokolldaten der Endbenutzer im Namen ihrer Kunden, wenn deren Endbenutzer gemäß der Genehmigung unserer Kunden auf unsere Dienste zugreifen. Diese verarbeiteten Protokolldaten können unter anderem IP-Adressen, Systemkonfigurationsinformationen und andere Informationen über den ein- und ausgehenden Traffic von den Websites, Geräten, Anwendungen und/oder Netzwerken unserer Kunden umfassen. Unsere Datenschutzrichtlinie beschreibt, welche Informationen wir erheben und wie wir diese gesammelten Informationen verwenden. Darüber hinaus erhebt und speichert Cloudflare als Datenverantwortlicher Daten zur Server- und Netzwerkaktivität und Protokolle im Laufe des Betriebs des Dienstes. Zudem werden Beobachtungen und Analysen von Verkehrsdaten durchgeführt (wir sprechen dabei von „Betriebskennzahlen“). Beispiele für Betriebskennzahlen sind Daten zur Service-Betriebszeit und Service-Verfügbarkeit, Anfragevolumen, Fehlerquoten, Cache-Raten und IP-Bedrohungsbewertungen.

Wenn wir Daten aus Aktivitäten in unserem Netzwerk erheben und speichern, tun wir dies nur, um unsere Produkte für Sie, unsere anderen Kunden oder die Internet-Gemeinde im Allgemeinen zu verbessern. Wir können zum Beispiel Netzwerkverkehrsdaten aller unserer Kunden weltweit vorübergehend speichern und analysieren, um die Endnutzer auf intelligente Weise über die am wenigsten überlasteten und zuverlässigsten Wege durch das Internet zu leiten. Wir speichern möglicherweise auch Netzwerkdaten und analysieren sie, um aufkommende Bedrohungsvektoren zu erkennen und zu identifizieren. Auf diese Weise können wir den Schutz Ihrer Internetwebsites durch unsere Produkte sofort aktualisieren. Und schließlich können wir Netzwerkdaten großer Segmente unserer Kunden zusammenfassen (jedoch niemals von individuell identifizierbaren Benutzern oder Kunden), um der Internet-Gemeinde zu helfen, Erkenntnisse, Bedrohungen und Trends im Internet zu verstehen (siehe Cloudflare Radar). Letztlich werden die von uns erhobenen und gespeicherten Netzwerkdaten nur dazu verwendet, unser Netzwerk und unsere Produkte für unsere Kunden zu verbessern oder um aggregierte Internet-Trends mit der Internet-Gemeinde im Allgemeinen zu teilen.

Im Folgenden finden Sie einige der Datenschutzverpflichtungen, die wir eingehen und die uns von vielen anderen Cloud-Providern unterscheiden:

- Cloudflare verkauft keine personenbezogenen Daten.
- Wir verfolgen die Endnutzer unserer Kunden nicht über verschiedene Internetwebsites hinweg.
- Wir erstellen keine Profile der Endnutzer unserer Kunden, um Anzeigen zu verkaufen.
- Cloudflare bewahrt personenbezogene Daten nur dann auf, wenn dies erforderlich ist, um unseren Kunden Cloudflare-Angebote bereitzustellen.
- Cloudflare hat niemals die Verschlüsselungscodes von Kunden oder einen Feed mit Kundeninhalten, die unser Netzwerk durchlaufen, an Dritte oder Behörden weitergegeben. Wir haben uns seit langem verpflichtet, alle Rechtsmittel auszuschöpfen, bevor wir einer entsprechenden Anfrage nachkommen.
- Cloudflare hat öffentlich zugesagt, dass wir Rechtsmittel einlegen werden, um jede Anfrage der US-Regierung nach Daten anzufechten, die unserer Meinung nach der DSGVO unterliegen.
- Cloudflare wendet das Prinzip an, dass wir unsere Kunden über jeden rechtlichen Vorgang informieren, im Rahmen dessen ihre Informationen angefordert werden, bevor wir diese Informationen offenlegen – es sei denn, dies ist gesetzlich untersagt.

Cloudflare-Produktfunktionen zur Unterstützung des Datenschutzes

Unsere europäischen Kunden nutzen häufig die folgenden Funktionen zur Konfiguration ihrer Cloudflare-Implementierung, um ihren rechtlichen Verpflichtungen bezüglich des Umgangs mit Daten nachzukommen:

Dashboard und Portal-Sicherheit:
Das Cloudflare Dashboard bietet eine einfach zu bedienende Benutzeroberfläche, mit der Kunden alle von ihnen verwendeten Produkte, die im Cloudflare-Netzwerk laufen, konfigurieren und verwalten können. Kunden melden sich über die sicheren Webportale von Cloudflare beim Cloudflare Dashboard an. Um unseren Kunden einen sicheren und autorisierten Zugriff auf ihre Cloudflare-Konten und -Daten zu ermöglichen, haben wir Standard-Sicherheitsmerkmale in unsere Portale und das Dashboard eingebaut. Wir haben beobachtet, dass viele Unternehmen und Organisationen Schwierigkeiten haben, den Zugang zu ihren verschiedenen Sicherheitsvorrichtungen, Produkten und Diensten umfassend abzusichern. Im Gegensatz dazu basieren die Cloudflare-Produkte auf einer einzigen, einheitlichen und sicheren Plattform, sodass Cloudflare-Kunden von einem konsistenten und hochsicheren Kontozugriff für alle ihre Produkte zur Gewährleistung von Sicherheit, Performance und Zuverlässigkeit profitieren.

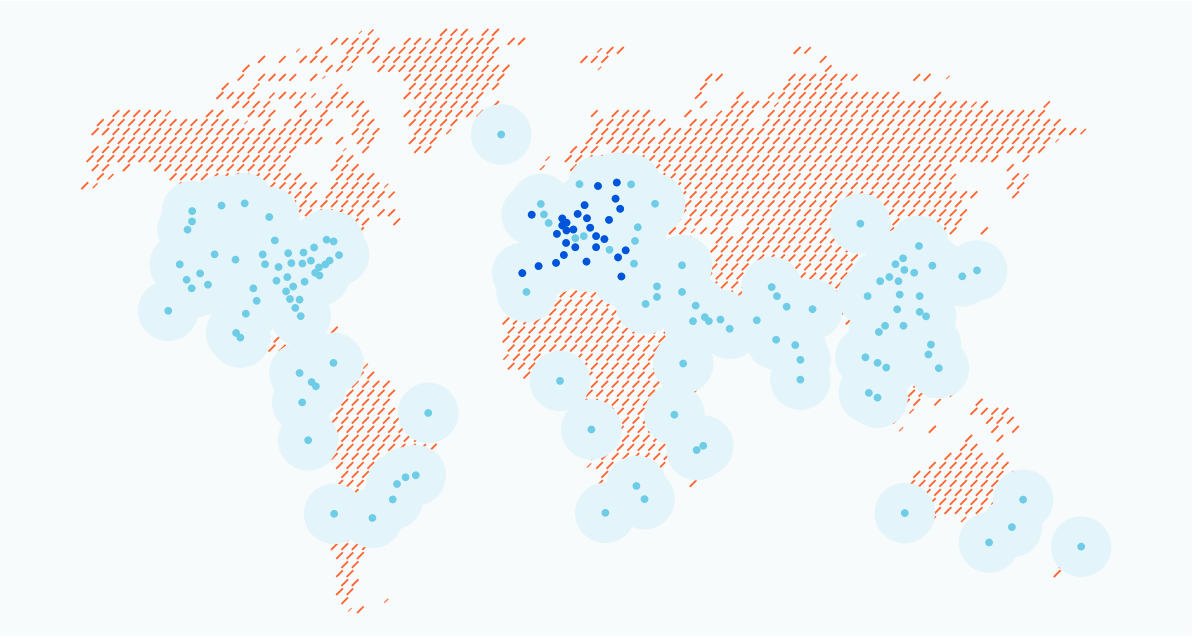
- **Zwei-Faktor-Authentifizierung** (2FA) verbessert die Kontosicherheit, indem beim Anmelden eine zweite Information zur Überprüfung der Benutzeridentität verlangt wird. Cloudflare 2FA unterstützt Hardware-Token und TOTP-Mobilfunkapplikationen.
- **Single-Sign-On** ermöglicht Kunden (wenn aktiviert) den Einsatz eines lokalen oder in der Cloud gehosteten Identitätsanbieters für die Zugriffskontrolle. Die vollständige Liste der unterstützten Provider finden Sie hier.
- **Audit-Protokolle** fassen den Verlauf des Zugriffs und die Änderungen an der Cloudflare-Konfiguration eines Kunden zusammen. Audit-Protokolle umfassen Aktionen auf Kontoebene wie das An- und Abmelden sowie Einstellungsänderungen an DNS, Crypto, Firewall, Speed, Caching, Page Rules, Netzwerk- und Traffic-Funktionen usw. Audit-Protokolle sind für alle Tarifarten verfügbar und werden sowohl für einzelne Benutzer als auch für Organisationen mit mehreren Benutzern erfasst.

Verschlüsselung:
Verschlüsselung ist eine Möglichkeit, Daten so zu chiffrieren, dass nur autorisierte Parteien die Informationen verstehen können. Daten können „im Ruhezustand" bei der Speicherung verschlüsselt werden oder „während der Übertragung", wenn sie an einen anderen Ort übertragen werden. Die Verschlüsselung von Daten, die über ein Netzwerk übertragen werden, erfordert die Verwendung eines Verschlüsselungscodes. Dabei handelt es sich um eine Reihe mathematischer Werte, die sowohl dem Absender als auch dem Empfänger einer verschlüsselten Nachricht bekannt sind.

Durch die Verschlüsselung wird verhindert, dass Unbefugte – ob Angreifer, Anzeigennetzwerke, Internet-Service-Provider oder feindliche ausländische Akteure – sensible Daten abfangen und lesen. Durch verschlüsselte Kommunikation können die kommunizierenden Parteien sensible Daten austauschen, ohne dass diese nach außen dringen. Verschlüsselung trägt auch dazu bei, böswilliges Verhalten wie etwa Angriffe während des Transfers (On-Path-Angriffe) zu verhindern. Viele Branchen- und Regierungsvorschriften verlangen von Unternehmen, die mit Nutzerdaten umgehen, dass diese Daten verschlüsselt bleiben. Beispiele für Regulierungs- und Compliance-Standards, die eine Verschlüsselung erfordern, sind HIPAA, PCI-DSS und die DSGVO.

Cloudflare bietet die sichersten und leistungsstärksten Network-as-a-Service-Produkte, da wir Ihren gesamten Datenverkehr direkt vom Rand unseres Netzwerks durch Proxy-Server leiten. Als Ihr autorisierter Proxy-Anbieter überprüfen wir Ihren Datenverkehr sicher, um Bedrohungen zu identifizieren und ihn von jedem beliebigen Ort in unserem globalen Netzwerk aus weiterzuleiten. Mit Cloudflare haben Sie vollständige Kontrolle darüber, wo und wie der Datenverkehr überprüft wird. Cloudflare ist einer der wenigen Cloud-Provider, der als einheitliche globale Plattform konzipiert ist und auch für bestimmte regionale Anforderungen konfiguriert werden kann.

Regionale Dienste geben Organisationen die Kontrolle darüber, wo ihr Datenverkehr überprüft wird. Wenn die regionalen Dienste aktiviert sind, wird der Content-Verkehr über das globale Anycast-Netzwerk von Cloudflare an dem Standort aufgenommen, der dem Client am nächsten liegt. Statt am betreffenden Point of Presence (PoP) überprüft zu werden, wird dieser Datenverkehr sicher an Cloudflare-PoPs innerhalb der vom Kunden ausgewählten Region(en) übertragen, wo er dann abgewickelt wird. Wenn darüber hinaus „Geo Key Manager" angewendet wird, werden die TLS-Schlüssel des Kunden nur zur Abwicklung des Content-Verkehrs innerhalb dieser Regionen gespeichert und verwendet. „Regionale Dienste" hilft Kunden, die die lokale Kontrolle über ihren Traffic behalten und gleichzeitig die Sicherheitsvorteile eines globalen Netzwerks nutzen möchten.



Zum Beispiel kann ein Cloudflare-Kunde in Deutschland „Regionale Dienste“ aktivieren, um den Service auf die Europäische Union zu beschränken. Seine Endnutzer-Clients stellen eine Verbindung zum nächstgelegenen Cloudflare-Standort auf der ganzen Welt her. Wenn sich dieser Standort jedoch außerhalb der EU befindet, wird der Datenverkehr vor der Überprüfung an einen Cloudflare-Standort innerhalb der EU weitergeleitet. Der Kunde profitiert nach wie vor von unserem globalen Netzwerk mit niedriger Latenz und hohem Durchsatz, das selbst den größten DDoS-Angriffen standhält. Die regionalen Dienste geben den Kunden jedoch auch die lokale Kontrolle. Nur Rechenzentren innerhalb der EU haben den erforderlichen Zugang, um Sicherheitsrichtlinien anzuwenden. Dieser Ansatz ermöglicht es Cloudflare, den schnellsten Weg in die EU und den nächstgelegenen verfügbaren Point of Presence für die Bearbeitung zu wählen.

Cloudflare legt nicht nur fest, wo der Datenverkehr überprüft wird, sondern hilft Unternehmen auch dabei, Benutzer und Daten durch den Einsatz branchenführender Verschlüsselungstechniken und -technologien zu schützen. Mit „Geo Key Manager“ und „Keyless SSL“ haben Kunden die volle Kontrolle darüber, wo Schlüssel gespeichert sind und welche PoPs Zugriff auf diese Schlüssel haben.

Keyless SSL ermöglicht einem Kunden, seine eigenen privaten SSL-Schlüssel zur Verwendung mit Cloudflare zu speichern und zu verwalten. Kunden können eine Vielzahl von Systemen für ihren Keystore verwenden, darunter Hardware-Sicherheitsmodule („HSMs“), virtuelle Server und Hardware unter Unix/Linux und Windows, die in Umgebungen untergebracht ist, die der Kunde kontrolliert. „Keyless SSL“ setzt mehrere Methoden ein, um eine sichere Verbindung für die Schlüsselübertragung vom Kunden zu Cloudflare zu schaffen. Zudem bietet sie eine Sitzungspersistenz, die in der Regel die Gesamtgeschwindigkeit von SSL-Transaktionen beschleunigt.

Geo Key Manager bietet Kunden eine genaue Kontrolle darüber, wo ihre Schlüssel gespeichert werden. Beispielsweise kann ein Kunde entscheiden, dass die privaten Schlüssel nur innerhalb von PoPs in der EU zugänglich sind.

Mit Cloudflare haben Kunden weitreichende Kontrolle nicht nur darüber, wo private Schlüssel gespeichert werden, sondern auch darüber, wo der Datenverkehr tatsächlich auf Sicherheitsbedrohungen untersucht wird. Wenn ein Kunde es wünscht, können nur PoPs innerhalb der EU-Mitgliedsstaaten den Verkehr inspizieren.

Die globalen und europäischen Sicherheitszertifizierungen von Cloudflare

Cloudflare erfüllt branchenweit führende Standards für Sicherheit und Datenschutz und validiert diese Verpflichtungen jährlich mit externen Prüfern. Cloudflare ist konform mit ISO 27001/27002, Payment Card Industry Data Security Standards (PCI DSS) und SSAE 18 SOC 2 Type II. Wir haben Geschäftspartner-Vereinbarungen unterzeichnet und sind in der Lage, Unternehmen zu unterstützen, die dem Health Insurance Portability and Accountability Act von 1996 (HIPAA) unterliegen. Diese Validierungen bieten Unternehmen, die ihre sensibelsten Daten über unsere Dienste übertragen, Sicherheit und helfen ihnen auch dabei, ihre eigenen Compliance-Verpflichtungen zu erfüllen und einzuhalten.

Zusätzlich zu den regelmäßigen Bewertungen durch Dritte anhand von Industriestandards gilt Cloudflare als „Betreiber wesentlicher Dienste" im Sinne der EU-Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie). Neben der Registrierung gemäß dieser Richtlinie bei ICO und Ofcom in Großbritannien, BSIG in Deutschland und CNCS in Portugal wurde Cloudflare auch im Hinblick auf spezifische regionale Anforderungen, wie etwa das BSI-Gesetz in Deutschland (BSIG), bewertet. Wir pflegen unsere Beziehungen zu den europäischen Regionalbehörden und arbeiten eng mit ihnen zusammen, wenn es um die Einhaltung der Vorschriften geht. Zudem geben wir Einblicke, wie wir den Datenschutzanforderungen gerecht werden.

Auf praktischer Ebene stellte der europäische Wendepunkt, die Datenschutz-Grundverordnung (DSGVO), eine Kodifizierung vieler der Schritte dar, die wir bereits unternommen hatten:

- Cloudflare erhebt nur die personenbezogenen Daten, die wir benötigen, um den von uns angebotenen Dienst zu erbringen.
- Cloudflare verkauft keine personenbezogenen Daten.
- Cloudflare gibt Personen die Möglichkeit, auf ihre personenbezogenen Daten zuzugreifen, sie zu korrigieren oder zu löschen.
- In Übereinstimmung mit unserer Rolle als Auftragsverarbeiter gibt Cloudflare Kunden die Kontrolle über die Informationen, die zum Beispiel in unserem Content Delivery Network (CDN) zwischengespeichert, im Workers Key Value Store gespeichert oder von unserer Web Application Firewall (WAF) erfasst werden.

Unsere FAQ zur DSGVO finden Sie hier: cloudflare.com/de-de/gdpr/introduction.

Da uns Datenschutz wichtig ist, prüfen wir nicht nur dort, wo wir gesetzlich dazu verpflichtet sind oder wo Zertifikate vorliegen. Unser Sicherheitsteam führt strenge interne und externe Penetrationstests durch, wir betreiben über HackerOne ein Bug-Bounty-Programm und wir beauftragen externe Prüfer, um die Einhaltung unserer Datenschutzverpflichtungen zu bestätigen. Starke Beispiele sind datenschutzorientierte Audits, wie wir sie Anfang dieses Jahres in Bezug auf unsere Verpflichtungen für unseren 1.1.1.1 öffentlichen DNS-Resolver durchgeführt haben. Wir sind immer offen für zusätzliche Validierungen, die Sicherheit für unser Datenschutzprogramm, unsere Richtlinien und unsere Verfahren zur Verarbeitung und Speicherung personenbezogener Daten in der EU bieten.

Die Datenübertragungs-Mechanismen von Cloudflare

Welche Arten von personenbezogenen Daten Cloudflare im Auftrag eines Kunden verarbeitet, hängt davon ab, welche Cloudflare-Dienste implementiert sind. Die überwiegende Mehrheit der Daten, die das Cloudflare-Netzwerk durchlaufen, verbleibt auf den Edge-Servern von Cloudflare, während Protokolldaten zu dieser Aktivität im Auftrag unserer Kunden in unserem zentralen Rechenzentrum in den USA verarbeitet werden können – selbst wenn Kunden „Regionale Dienste" aktivieren.

Einige dieser Protokolldaten enthalten Informationen über Besucher und autorisierte Benutzer der Domains, Netzwerke, Websites, Anwendungs-Programmierschnittstellen („APIs") oder Anwendungen unserer Kunden. Diese Metadaten enthalten in äußerst begrenztem Umfang personenbezogene Daten, meist in Form von IP-Adressen. Wir verarbeiten diese Art von Informationen im Auftrag unserer Kunden in unserem Hauptrechenzentrum in den USA für einen begrenzten Zeitraum.

Da personenbezogene Daten in begrenztem Umfang in die USA übertragen werden, haben wir es Unternehmen leicht gemacht, bei der Nutzung von Cloudflare-Services einen gültigen Datenübertragungs-Mechanismus aufrechtzuerhalten. Unser Standard-Auftragsverarbeitungsvertrag (Data Processing Agreement – DPA) ist in unserer Enterprise-Servicevereinbarung enthalten und der DPA beinhaltet die EU-Standardvertragsklauseln (Standard Contractual Clauses – SCCs) für betroffene Personen, die der DSGVO unterliegen. Insgesamt gewährleisten die Bedingungen von Cloudflare ein Schutzniveau für personenbezogene Daten, das dem durch die DSGVO garantierten Schutzniveau entspricht. Weitere Informationen über unser Engagement für die DSGVO und über unseren DPA finden Sie hier.

Am 16. Juli 2020 erließ der Gerichtshof der Europäischen Union („EuGH“) eine Entscheidung, die das EU-US Privacy Shield im Fall „Schrems II“ für ungültig erklärte. Infolgedessen haben uns einige unserer Kunden, die die Daten von in der EU ansässigen Personen verarbeiten, die Frage gestellt, was diese Entscheidung für die Rechtmäßigkeit der Übertragung von Daten in die USA bedeutet, die von Cloudflare in ihrem Auftrag verarbeitet werden. Erstens ändert die Außerkraftsetzung des Privacy Shield nichts an den starken Datenschutzvorkehrungen, die Cloudflare für die personenbezogenen Daten, die wir im Auftrag unserer Kunden verarbeiten, getroffen hat. Wir werden weiterhin die Datenschutzgrundsätze befolgen, zu denen wir uns bei der Zertifizierung im Rahmen des Privacy Shield verpflichtet haben.

Nach dem Beschluss Schrems II bleiben die von der EU zugelassenen SCCs ein gültiger Transfermechanismus gemäß der DSGVO, wobei zusätzliche Sicherheitsvorkehrungen auch für Daten gelten, die in die USA übermittelt werden. Cloudflare wird weiterhin den SCCs-Mechanismus für Datentransfers nutzen und wir haben unseren Standard-Kunden-DPA aktualisiert, um zusätzliche Sicherheitsvorkehrungen als vertragliche Verpflichtungen aufzunehmen. Zum Beispiel verpflichten wir uns, Rechtsmittel einzulegen, um jede Anfrage der US-Regierung nach Daten anzufechten, die wir als unter den Geltungsbereich der DSGVO-fallend identifizieren. Darüber hinaus verpflichten wir uns, unsere Kunden über alle rechtlichen Verfahren zu informieren, in deren Rahmen ihre Daten angefordert werden, bevor diese Daten offengelegt werden – sofern dies nicht gesetzlich verboten ist. Sie können die zusätzlichen Schutzmaßnahmen, die wir als vertragliche Verpflichtungen hinzugefügt haben, in Abschnitt 7 unseres DPA nachlesen.

Datenschutzbestimmungen und -richtlinien entwickeln sich ständig weiter und wir beobachten die Regulierungs- und Gesetzgebungslandschaft genau. Wir behalten ständig neue Leitlinien im Auge, um sicherzustellen, dass unsere Kunden und Partner weiterhin die Vorteile von Cloudflare in ganz Europa genießen können.

Gemeinsame Chancen und Verantwortlichkeiten

Da wir wissen, dass alle europäischen Organisationen Datenschutz- und Sicherheitsprinzipien in jede Phase ihrer Geschäftstätigkeit integrieren müssen, haben wir dieses Diagramm erstellt, damit Sie leicht nachvollziehen können, wer für diese allgemein geforderten Datenschutzanforderungen verantwortlich ist:

Prinzip	Verantwortung	Einzelheiten zur Verantwortung
Datenschutz durch Design	Gemeinsam genutzt	Cloudflare ist verantwortlich für die Bereitstellung von Produkten und Dienstleistungen unter Berücksichtigung des Datenschutzes. Das Datenschutzteam bietet Überprüfungen, Beurteilungen und Schulungen an, um sicherzustellen, dass der Datenschutz in unserer Arbeitsweise berücksichtigt wird. Kunden sind für die Nutzung und Konfiguration ihrer Cloudflare-Dienste verantwortlich und sollten die Nutzung und Konfiguration dieser Dienste regelmäßig überprüfen, um sicherzustellen, dass die Datenschutzprinzipien bei der Konzeption und Implementierung berücksichtigt wurden.
Antrag auf Zugriff durch betroffene Personen	Gemeinsam genutzt	Cloudflare bietet betroffenen Personen bei Datenschutzverletzungen das Recht auf Zugang, Korrektur und Löschung von personenbezogenen Informationen unabhängig von der Gerichtsbarkeit ihres Wohnsitzes. Anfragen von betroffenen Personen können an sar@cloudflare.com gesendet werden. Wenn wir eine Anfrage von jemandem erhalten, der ein Endbenutzer eines unserer Kunden zu sein scheint, werden wir diese Person anweisen, sich direkt mit diesem in Verbindung zu setzen.

Prinzip	Verantwortung	Einzelheiten zur Verantwortung
Angemessene Sicherheit	Gemeinsam genutzt	Cloudflare unterhält ein Sicherheitsprogramm, das den Branchenstandards entspricht. Das Sicherheitsprogramm umfasst die Aufrechterhaltung formaler Sicherheitsrichtlinien und -verfahren, die Einrichtung angemessener logischer und physischer Zugangskontrollen, die Implementierung technischer Schutzmaßnahmen in Unternehmens- und Produktionsumgebungen (einschließlich der Einrichtung sicherer Konfigurationen, sicherer Übertragung und Verbindungen, Protokollierung und Überwachung) und die Bereitstellung angemessener Verschlüsselungstechnologien für personenbezogene Daten. Kunden sind dafür verantwortlich, die Sicherheitslage ihrer Cloud-Provider wie Cloudflare zu überprüfen, und können dies tun, indem sie unsere Compliance-Validierungen und Berichte einsehen. Wir ermutigen unsere Kunden auch, ihre Dashboard-Sicherheitseinstellungen zu überprüfen, um sicherzustellen, dass sie ihre Sicherheitsrichtlinien und -abläufe befolgen.
Rechtliche Grundlage für die Verarbeitung	Gemeinsam genutzt	Cloudflare verarbeitet Daten gemäß den Anweisungen unserer Kunden, den für die Datenverarbeitung Verantwortlichen, und arbeitet als DSGVO-konformer Datenverarbeiter. Kunden sind dafür verantwortlich, sicherzustellen, dass sie über eine angemessene rechtliche Grundlage für die Verarbeitung der Daten ihrer Endbenutzer verfügen.
Verletzungen personenbezogener Daten	Gemeinsam genutzt	Cloudflare benachrichtigt Kunden, sobald wir von einer Sicherheitsverletzung Kenntnis erlangen, die zum Verlust, zur unberechtigten Offenlegung von oder zum unberechtigten Zugang zu personenbezogenen Daten führt, die von Cloudflare oder Subunternehmen der Firma verarbeitet werden. Cloudflare ist auch dafür verantwortlich, unseren Kunden eine angemessene Zusammenarbeit und Unterstützung im Hinblick auf die Sicherheitsverletzung zu bieten, einschließlich der Bereitstellung angemessener Informationen im Besitz von Cloudflare über die Umstände der Sicherheitsverletzung und die betroffenen personenbezogenen Daten. Kunden sind dafür verantwortlich, die gesetzlichen oder vertraglichen Anforderungen zu erfüllen, um ihre Endnutzer und/oder staatliche Stellen über jegliche Verletzung personenbezogener Daten zu informieren.

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

Oberste Priorität von Cloudflare ist es, das Vertrauen der Kunden zu gewinnen und zu bewahren. Wir sind uns bewusst, dass Transparenz bei den Datenschutzverpflichtungen von Cloudflare und bei unserem Ansatz, Datenlokalisierung und Datenschutz in unser Netzwerk und unsere Produkte zu integrieren, Kunden hilft, ihren eigenen Verpflichtungen nachzukommen. Wir wissen auch, dass unsere Branchenzertifizierungen und wohl durchdachten Vertragsmechanismen uns helfen, ein starkes Vertrauensverhältnis zu unseren europäischen Kunden aufzubauen.

Unsere Datenschutz- und Sicherheitsteams sind bereit, gemeinsam mit Ihnen die strengsten Anforderungen zu erfüllen, mit denen Sie in Ihrem Land, Ihrer Region oder Ihrer Branche konfrontiert werden können. Unsere sachkundigen Kundenbetreuer, Customer Success-Manager und Vertriebsingenieure arbeiten regelmäßig mit unseren Datenschutz- und Sicherheits-Compliance-Teams zusammen, um unsere Kunden bei der Konfiguration der Cloudflare-Produkte zu unterstützen, die sie zur Erfüllung ihrer konkreten Compliance-Verpflichtungen verwenden. Wenn Sie eine Demo oder eine spezialisierte Sitzung zur Konfiguration Ihrer Dienstleistungen wünschen, um Ihren besonderen Verpflichtungen nachzukommen, kontaktieren Sie uns noch heute. Bitte senden Sie uns eine E-Mail an privacyquestions@cloudflare.com oder security@cloudflare.com.

WEITERE INFORMATIONEN

1. **Die Protokolldienste von Cloudflare verstehen**
2. **Verwalten und Analysieren von Protokollen**
3. **FAQs zu Protokollen**
4. **Kontaktieren Sie uns,** um regionale Dienste zu aktivieren