CLOUDFLARE

WHITEPAPER

Cloudflare-Richtlinien für Datenschutz und Anfragen von Strafverfolgungsbehörden

Veröffentlicht am 28. Januar 2021

Übersicht

Das Vertrauen unserer Kunden bildet das Fundament für das Cloudflare-Netzwerk und unsere Geschäftsaktivitäten. Um diesem Vertrauen gerecht zu werden und es zu bewahren, entwickeln und verwenden wir Produkte, die die Sicherheit unserer eigenen Systeme erhöhen und Daten im Ruhezustand oder bei der Übertragung verschlüsseln. Außerdem können unsere Kunden bestimmen, wie Traffic an verschiedenen Standorten rund um den Globus geprüft wird.

Doch nicht alle Herausforderungen lassen sich auf technischem Weg lösen. Deshalb verfügen wir über Richtlinien und Verfahren zur Verwaltung der Kunden- und Endnuzterdaten in unseren Systemen und zum Umgang mit behördlichen und anderen rechtlich zulässigen Datenanfragen.

Im folgenden Text werden diese Richtlinien beschrieben. Außerdem finden sich darin Links zu weiterführenden Informationen über verschiedene Aspekte unseres Datenschutz- und Compliance-Konzepts. Im Besonderen wird in dem Text Folgendes abgedeckt:

- Unsere Sicht auf die sich verändernde Datenschutzlandschaft
- Unsere Richtlinien für Datenschutz und Datenanfragen

Die sich verändernde Datenschutzlandschaft

Die explosionsartige Ausbreitung von Cloud-Diensten und die Tatsache, dass Daten gegebenenfalls außerhalb des Wohnsitzlandes derjenigen gespeichert werden, die sie generiert haben, stellt für ermittelnde Strafverfolgungsbehörden eine Herausforderung dar. Online-Service-Provider aller Art dienen oft als Zugangspunkt zu diesen elektronischen Aufzeichnungen.

Für Service-Provider wie Cloudflare können solche Anfragen heikel sein. Einerseits leisten Strafverfolgungsbehörden und andere staatliche Stellen wichtige Arbeit. Andererseits sind die bei uns angeforderten Daten nicht unser Eigentum. Wenn Kunden unsere Dienste nutzen, haben sie uns diese Daten anvertraut. Dieses Vertrauen zu bewahren, ist sowohl für unser Geschäft als auch für unsere Werte von maßgeblicher Bedeutung.

Verstärkt wird dieses Spannungsfeld noch durch die Tatsache, dass Regierungen unterschiedliche Standards für den Schutz personenbezogener Daten festgelegt haben. Die Vereinigten Staaten beispielsweise verbieten Unternehmen, den Inhalt von Mitteilungen – auch gegenüber Regierungen anderer Länder – offenzulegen, sofern nicht ganz bestimmte, gesetzlich eingegrenzte Umstände gegeben sind. Die Europäische Union (EU), die Datenschutz seit langem als grundlegendes Menschenrecht betrachtet, schützt alle personenbezogenen Daten innerhalb ihres Gebiets durch die Datenschutz-Grundverordnung (DSGVO). Diese Vorschriften überlappen zwar, unterscheiden sich aber sowohl in ihrem Umfang als auch darin, wen sie schützen.

Die Unterschiede zwischen den rechtlichen Rahmenordnungen sind von Bedeutung – insbesondere wenn es darum geht, ob die rechtlichen Informationsanfragen ausländischer Regierungen mit den Datenschutzvorschriften in Einklang stehen. In den letzten Jahren ist der Europäische Gerichtshof (EuGH) zum Beispiel mehrfach zu dem Schluss gekommen, dass die rechtlichen Beschränkungen der Vereinigten Staaten für die Datenerhebung zusammen mit bestimmten freiwilligen Verpflichtungen wie dem „Privacy Shield“ oder seinem Vorgänger, dem „U.S.-EU Safe Harbor“, den Datenschutzanforderungen der EU nicht genügen. Das ist in erster Linie aufgrund der US-Gesetze der Fall, die es den Justizbehörden erlauben, Informationen über Nicht-US-Bürgerinnen und -Bürger zur Verwendung des Auslandsgeheimdienstes zu sammeln. In der Tat vertritt der Europäische Datenschutzausschuss (European Data Protection Board – EDPB) die Position, dass eine strafrechtsbezogene Datenanfrage durch US-Behörden – die nicht Teil eines rechtlichen Verfahrens ist, bei dem Länder in der EU eine gewisse Kontrolle über die herausgegebenen Informationen behalten – keine legitime Grundlage für die Übermittlung personenbezogener Daten darstellt, die der DSGVO unterliegen.

Im Kern geht es um die Frage, wann es für eine Regierung angemessen ist, Rechtsanordnungen oder andere rechtliche Verfahren einzusetzen, um auf Daten von Bürgerinnen und Bürgern eines anderen Landes zuzugreifen. Dieser Konflikt besteht auch keineswegs nur in Europa. Immer mehr Länder den Zugang zu den Daten ihrer Bürgerinnen und Bürger inzwischen als eine Frage der nationalen Sicherheit, auch wenn sie unterschiedliche Maßnahmen zu ihrem Schutz ergreifen.

Cloudflare-Richtlinien für Datenschutz und Datenanfragen

Cloudflare wendet bereits seit längerer Zeit Richtlinien an, die sich der Bedenken bezüglich des Zugangs zu personenbezogenen Daten annehmen. Einerseits hielten wir das für richtig und andererseits erschienen uns die heutigen rechtlichen Konflikte schon damals unausweichlich. Diese Richtlinien umfassen:

- Öffentliche Zusagen hinsichtlich des Umgangs mit vertraulichen Daten und entsprechenden Datenanfragen von Strafverfolgungsbehörden
- Die Art und Weise, in der wir unsere Kunden über Datenanfragen informieren

Wenn zwei Normen miteinander in Konflikt stehen, halten wir uns generell an diejenige, die den besten Datenschutz gewährleistet. Wir verlangen zudem immer die Einhaltung eines ordnungsgemäßen rechtlichen Verfahrens. Denn wurde einmal Zugang zu Daten gewährt, lässt sich das oft nur schwer wieder rückgängig machen.

Unsere öffentlichen Zusagen hinsichtlich Datenschutz und Anfragen von Strafverfolgungsbehörden

Seit unserem ersten Transparenzbericht im Jahr 2013, in dem Datenanfragen von Strafverfolgungsbehörden aufgeführt wurden, haben wir nicht nur öffentliche Zusagen hinsichtlich unseres Umgangs mit Datenanfragen gemacht, sondern auch öffentliche Stellungnahmen zu den Dingen abgegeben, die wir nie getan haben. Die zweite Art der Meldung bezeichnen wir als „Warrant Canary“, die – ähnlich wie früher Kanarienvögel im Bergbau – eine Warnfunktion für die Außenwelt haben soll.

Sie erfüllt zwei Aufgaben: Erstens versichern wir damit öffentlich, dass wir die entsprechenden Maßnahmen nicht freiwillig ergreifen würden. Zweitens kann die Entfernung einer solchen Stellungnahme von der Website der Übermittlung von Informationen dienen, die wir andernfalls möglicherweise nicht offenlegen dürften.

Aufsichtsbehörden haben begonnen, den Wert von Datenschutzverpflichtungen anzuerkennen, insbesondere wenn sie vertraglich durchgesetzt werden können. In der Tat entsprechen die Verpflichtungen, die seit Jahren in unseren Transparenzberichten enthalten sind, genau denen, die von der Europäischen Kommission in ihrem Entwurf für Standardvertragsklauseln zur Einhaltung der DSGVO empfohlen werden.

Einige unserer wichtigsten Zusagen zum Zeitpunkt der Veröffentlichung dieses Texts:

- **Wir haben niemals Software oder Geräte von Strafverfolgungsbehörden in unserem Netzwerk installiert oder einen Feed der Inhalte bereitgestellt, die unser Netzwerk durchlaufen**: Als Sicherheitsunternehmen wissen wir, dass die Kontrolle über den Zugang zu unseren Netzwerken eine absolute Notwendigkeit ist. Unser Sicherheitsteam hat sich aus diesem Grund auf Zugangskontrollen, Logging und Monitoring konzentriert. Außerdem wird es jährlich mehrfach einer externen Bewertung unterzogen. Wir möchten unseren Kunden vermitteln, dass bei diesen Kontrollen keine Ausnahmen für Strafverfolgungsbehörden oder andere staatliche Stellen gemacht werden. Daher versichern wir, dass niemals Strafverfolgungssoftware oder -ausrüstung im Cloudflare-Netzwerk installiert wurde und wir niemals Behörden einen Feed von Inhalten unserer Kunden zur Verfügung gestellt haben, die über unser Netzwerk übertragen wurden.
- **Wir haben niemals Kryptographie- oder Authentifizierungsschlüssel weitergegeben:** Cloudflare ist überzeugt, dass Online-Datenschutz eine starke Verschlüsselung – sowohl von Inhalten als auch von Metadaten – erfordert. Wenn ein Land verhindern will, dass ein anderes Zugriff auf die personenbezogenen Daten seiner Bürgerinnen und Bürger erhält, sollten zuerst diese Daten verschlüsselt werden. Aber Kundinnen, Kunden und Aufsichtsbehörden müssen sich auch darauf verlassen können, dass die Verschlüsselung selbst vertrauenswürdig ist. Wir versichern deshalb, dass wir niemals unsere Kryptographie- oder Authentifizierungsschlüssel oder die Kryptographie- oder Authentifizierungsschlüssel unserer Kundinnen und Kunden jemandem ausgehändigt haben und dass wir unsere Verschlüsselung niemals auf Ersuchen von Strafverfolgungsbehörden oder anderen Dritten abgeschwächt, beeinträchtigt oder unterlaufen haben.
- **Wir haben niemals Kundeninhalte oder DNS-Anfragen verändert:** Weitere Verpflichtungen, die Cloudflare eingegangen ist, beziehen sich auf die Integrität des Internets selbst. Unserer Auffassung nach sollten unsere Systeme nicht ausgenutzt werden, um Menschen zu Websites zu lotsen, die sie nicht besuchen wollten, oder um die Inhalte zu verändern, die sie online erhalten. Wir haben daher öffentlich erklärt, dass wir niemals Kundeninhalte verändert oder das beabsichtigte Ziel von DNS-Antworten auf Ersuchen von Strafverfolgungsbehörden oder anderen Dritten geändert haben.
- **Transparenz in Bezug auf mögliche Verstöße gegen unsere Verpflichtungen**: Wir haben uns verpflichtet, jede rechtliche Anordnung anzufechten, die darauf abzielt, dass wir diese Verpflichtungen nicht einhalten – notfalls auch vor Gericht. Damit wollten wir nicht nur gegenüber unseren Kundinnen und Kunden, sondern auch gegenüber Regierungen auf der ganzen Welt deutlich machen, wo wir unsere Grenzen ziehen.

Unsere allgemeine Einstellung im Hinblick auf Datenschutz hat sich seit unserer Gründung nicht geändert. Wir passen jedoch unsere Zusagen gelegentlich an, damit sie die neuesten Änderungen bei unseren Produkten und Richtlinien widerspiegeln. Eine endgültige und aktuelle Liste der von uns eingegangenen Verpflichtungen finden Sie auf der Seite zu unserem Transparenzbericht.

Benachrichtigung unserer Kunden über behördliche Anfragen

Cloudflare vertritt seit langem die Ansicht, dass unsere Kundinnen und Kunden berechtigt sind, darüber in Kenntnis gesetzt zu werden, wenn jemand – einschließlich einer Strafverfolgungsbehörde oder eines anderen staatlichen Akteurs – den Rechtsweg zur Anforderung ihrer Daten beschreitet. Auf diese Weise haben sie die Möglichkeit, bei Bedenken gegebenenfalls gegen die Anforderung vorzugehen.

Tatsächlich haben wir seit unseren Anfängen eine Firmenpolitik der Benachrichtigung unserer Kundinnen und Kunden verfolgt. Das FBI ist im Januar 2013, als wir noch keine 30 Mitarbeiter hatten, mit einer Verfügung (National Security Letter) bei uns erschienen, hat Informationen zu einem Kunden verlangt und uns untersagt, mit jemand anderem außer unseren Anwälten über die Angelegenheit zu sprechen. Solche Verfügungen unterlagen seinerzeit so gut wie keiner Kontrolle, konnten von einem einzigen Zweig der US-Regierung sowohl verfasst als auch vollstreckt werden und verpflichteten die Empfänger auf unbestimmte Zeit, Stillschweigen darüber zu bewahren.

Wir sind uns bewusst, dass es unter bestimmten Umständen zur Gewährleistung der Durchführbarkeit einer Untersuchung für Strafverfolgungsbehörden angemessen sein kann, die Offenlegung vorübergehend einzuschränken. Wir sind jedoch auch der Meinung, dass die Regierung verpflichtet sein sollte, jede Bestimmung zur Nichtoffenlegung zu rechtfertigen, und dass jede Bestimmung zur Nichtoffenlegung ausdrücklich auf den für den jeweiligen Zweck erforderlichen Mindestzeitraum begrenzt werden sollte. Aus diesem Grund haben wir gemeinsam mit der Electronic Frontier Foundation an einer rechtlichen Anfechtung des Schreibens gearbeitet. Das daraus resultierende Gerichtsverfahren erstreckte sich über mehrere Jahre und wir mussten bis 2017 Stillschweigen darüber bewahren. Letztendlich hat das FBI das Schreiben jedoch zurückgezogen.

US-Gerichte haben zu bedenken gegeben, dass unbegrenzte Verfügungen der Nichtoffenlegung verfassungsrechtliche Probleme aufwerfen. Deshalb hat das Justizministerium des Landes im Jahr 2017 Leitlinien veröffentlicht, in denen die Bundesstaatsanwälte angewiesen werden, Verfügungen zur Nichtoffenlegung außer in Ausnahmefällen auf maximal ein Jahr zu beschränken. Das hat jedoch nicht alle US-Strafverfolgungsbehörden davon abgehalten, sich um unbefristete Verfügungen zur Nichtoffenlegung zu bemühen. Tatsächlich haben wir nach Stand des Veröffentlichungsdatums dieses Texts seit 2017 mindestens 28 Verfügungen zur Nichtoffenlegung ohne Enddatum erhalten. In Zusammenarbeit mit der American Civil Liberties Union (ACLU) hat Cloudflare jeweils einen Rechtsstreit angedroht, wenn wir solche unbefristeten Verfügungen zur Nichtoffenlegung erhalten haben. In jedem dieser Fälle hat die Behörde nachträglich Fristen für die Nichtoffenlegung in diese Verfügungen eingefügt, sodass wir unsere Kundinnen und Kunden über die Anfragen informieren konnten.

Umgang mit Rechtskonflikten

Um die Einhaltung von Gesetzen wie der DSGVO zu gewährleisten, müssen Gerichte eingeschaltet werden – insbesondere angesichts von Rechtsanordnungen, die uns in die schwierige Lage bringen könnten, gegen solche Vorschriften verstoßen zu müssen. Ein Service-Provider wie Cloudflare kann ein Gericht bitten, rechtliche Anträge wegen eines Rechtskonflikts aufzuheben. Wir haben uns sowohl in unseren öffentlichen Erklärungen als auch vertraglich in unserem Datenverarbeitungszusatz (Data Processing Addendum) dazu verpflichtet, diesen Schritt zu unternehmen, falls dies zur Vermeidung eines solchen Konflikts erforderlich sein sollte. Wir sind der Ansicht, dass der Konflikt wieder dort ausgetragen sollte, wo er hingehört – zwischen den beiden Regierungen, die darüber streiten, wer das Recht auf Zugang zu Informationen haben soll.

Fazit

Dieser Texts bietet lediglich eine Übersicht über unsere umfassenden und weitreichenden Datenschutzverpflichtungen.

Hier können Sie sich näher über diese Verpflichtungen informieren:

- **Allgemeine Datenschutzrichtlinie**: Neben anderen häufig auftauchenden Datenschutzfragen wird darin erläutert, welche Daten wir erheben, wie wir sie verwenden und welche Daten wir weitergeben.
- **Transparenzbericht**: Aktuelle Informationen zu rechtlich zulässigen Anfragen bezüglich der Offenlegung von Informationen zu unseren Kunden, die wir erhalten haben.
- **Homepage zu Datenschutz und Compliance**: Die neuesten Stellungnahmen dazu, wie unsere Richtlinien und Produkte Datenschutz- und Compliance-Anforderungen erfüllen.

Letztlich müssen wir uns für den Betrieb eines globalen Netzwerks, das Kunden- und Endnutzerdaten schützt und mit den verschiedenen Datenschutzgesetzen rund um den Globus in Einklang steht, auf die Werte aus unseren frühsten Tagen zurückbesinnen: Prinzipientreue und Transparenz, Respekt der Privatsphäre, ordentliche Verfahren und rechtzeitige Mitteilungen an Kunden, damit diese selbst über ihre Daten entscheiden können.

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

REV:BDES-5987.2024JUL29