

WHITEPAPER

In che modo Cloudflare aiuta a far fronte agli obblighi in materia di protezione dei dati e località in Europa



Contenuto

- 3** Riepilogo
 - 4** **In che modo Cloudflare aiuta a far fronte agli obblighi in materia di protezione dei dati e località in Europa**
 - 5** Cloudflare in Europa
 - 5** L'impegno aziendale unico di Cloudflare per la privacy
 - 6** Certificazioni di sicurezza globali ed europee di Cloudflare
 - 7** I dati trattati da Cloudflare
 - 7** I meccanismi di trasferimento dei dati di Cloudflare
 - 8** Prodotti Cloudflare con funzionalità progettate per il supporto della localizzazione dei dati
 - 11** Opportunità e responsabilità condivise
 - 13** **Una rete cloud globale basata sulla fiducia dei clienti**
- 

Riepilogo

Cloudflare è stata fondata per aiutare le aziende e i loro utenti finali a sentirsi più sicuri su Internet. Siamo un'azienda incentrata sulla privacy e la nostra rete e tutti i nostri prodotti sono realizzati pensando alla protezione dei dati.

Cloudflare mantiene un'ampia gamma di tutele legali e contrattuali conformi al Regolamento generale sulla protezione dei dati (GDPR) dell'Unione europea (UE).

Cloudflare offre una suite di prodotti con varie funzionalità e protezioni tecniche per i clienti di Cloudflare che non desiderano che i loro dati lascino l'Europa.

In che modo Cloudflare aiuta a far fronte agli obblighi in materia di protezione dei dati e località in Europa

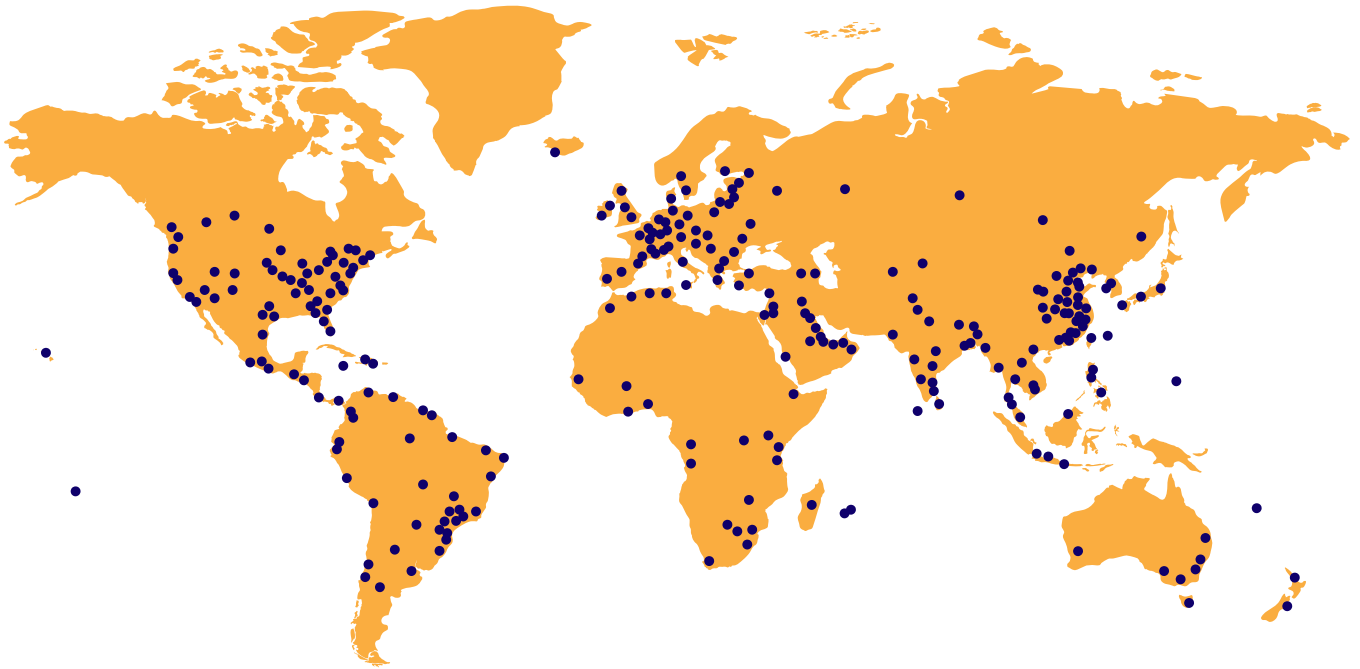


Figura 1: l'esclusiva rete cloud globale di Cloudflare è costituita da datacenter in oltre 250 città in più di 100 paesi. Cloudflare fornisce strumenti per gestire le modalità con cui i tuoi dati vengono instradati attraverso questi datacenter in modo da poter personalizzare dove viene ispezionato il traffico e quindi soddisfare le tue esigenze in termini di sicurezza, privacy e prestazioni.

Informazioni su Cloudflare

La missione di Cloudflare è aiutare a realizzare un Internet migliore. Forniamo una piattaforma cloud globale che offre un'ampia gamma di servizi di rete a privati e aziende di ogni dimensione in tutto il mondo. La rete di Cloudflare e il crescente portafoglio di prodotti migliorano la sicurezza, la privacy, le prestazioni e l'affidabilità di tutto quello che è connesso a Internet. Oltre a servire i nostri clienti, la missione di Cloudflare è anche aiutare a migliorare Internet stesso: sempre attivo, sempre veloce, sempre sicuro, sempre riservato e disponibile per tutti.

La rete, la community di sviluppatori e il business di Cloudflare sono tutti basati sulla fiducia dei clienti. Cerchiamo di guadagnare e mantenere

continuamente la fiducia dei clienti mostrando chiarezza sui nostri impegni in materia di privacy dei dati e su come gestiamo i dati dei clienti e degli utenti finali nei nostri sistemi. Creiamo fiducia anche realizzando e implementando prodotti che (i) contribuiscono a migliorare la sicurezza dei nostri sistemi, (ii) crittografano i dati inattivi o in transito e (iii) consentono ai nostri clienti di determinare come il traffico viene ispezionato in diverse località nel mondo. Infine, guadagniamo la fiducia dei clienti [proteggendo e mantenendo le certificazioni definite dal settore](#) (ad esempio, ISO 27001 e 27701, SSAE 18 e SOC 2 Type II) e fornendo meccanismi di contrattazione (ad esempio, Accordi sul trattamento dei dati) che comunicano il nostro modello di responsabilità condivisa con i nostri clienti nel garantire la privacy.

Cloudflare in Europa

Oggi, milioni di proprietà Internet in tutto il mondo utilizzano Cloudflare. Questo elenco include molte delle aziende più grandi e in più rapida crescita d'Europa, tra cui Eurovision, L'Oreal, AO.com, C&A, AllSaints e molti altri marchi noti. Include anche un elenco crescente di importanti istituzioni europee, tra cui INSEAD, Börse Stuttgart, IATA e Telefonica. Poiché le aziende e le organizzazioni di ogni dimensione si affidano sempre di più a Internet come piattaforma fondamentale per servire i propri clienti, utenti e stakeholder, stanno rapidamente adottando reti cloud sicure e affidabili come Cloudflare per proteggere le proprie applicazioni, infrastrutture e persone esposte a Internet da minacce di ogni tipo.

Riconosciamo che la protezione dei dati in Europa presenti tutta una serie di problematiche. Alcune di queste sono correlate al Regolamento generale sulla protezione dei dati (GDPR) dell'Unione europea (UE) e alla decisione della Corte di giustizia dell'UE nella causa "Schrems II" (causa C-311/18, Data Protection Commissioner v Facebook Ireland and Maximilian Schrems), l'ultima delle quali ha comportato ulteriori requisiti per le aziende che trasferiscono dati personali al di fuori dell'UE. Inoltre, una serie di settori estremamente regolamentati richiedono che tipi specifici di dati personali rimangano all'interno dei confini dell'UE.

In quanto tale, la piattaforma Internet di Cloudflare è progettata per supportare i settori europei più attenti alla privacy e regolamentati, inclusi i servizi finanziari, il settore pubblico, l'energia, i servizi pubblici, la vendita al dettaglio, il gaming e l'assistenza sanitaria. In Cloudflare, realizziamo i nostri prodotti per soddisfare i più elevati standard di sicurezza e privacy degli utenti e collaboriamo a stretto contatto con ciascuno dei nostri clienti europei per aiutarli a soddisfare gli obblighi di protezione dei dati associati alla loro località specifica e al segmento di settore. Otteniamo questo obiettivo attraverso un'ampia gamma di percorsi, tra cui:

- Il nostro impegno aziendale globale per la privacy
- Mantenere le certificazioni di sicurezza globali ed europee

- Mantenere i meccanismi di trasferimento dei dati conformi al GDPR
- Offrire prodotti con varie funzionalità che supportano la localizzazione dei dati

Questo documento spiega tali percorsi in dettaglio.

L'impegno aziendale unico di Cloudflare per la privacy

Cloudflare è stata fondata per aiutare te e i tuoi clienti a fruire di una maggiore sicurezza su Internet. Siamo un'azienda incentrata sulla privacy e la nostra rete e tutti i nostri prodotti sono realizzati tenendo conto della protezione dei dati. Nella nostra [Informativa sulla privacy](#) ci impegniamo a non vendere i dati personali che trattiamo per tuo conto o a non utilizzarli per scopi diversi dall'erogazione dei nostri servizi. Fin dall'inizio, non abbiamo mai disatteso questa promessa. In effetti, la nostra posizione sulla privacy è stata definita molto prima che i governi iniziassero a regolamentare la privacy in modi da esortare molte altre aziende tecnologiche ad aggiornare le proprie prassi per dare priorità alla privacy dei clienti e degli utenti. Non generiamo entrate dalla pubblicità, né profiliamo gli utenti finali dei nostri clienti o i dati degli utenti finali per alcuno scopo, tutte prassi considerate contrarie ai motivi per cui raccogliamo e conserviamo i dati personali che trattiamo per tuo conto.

Di seguito sono riportati alcuni degli impegni in materia di privacy che ci differenziano da molti altri fornitori di servizi cloud:

- Cloudflare non vende dati personali.
- Cloudflare non monitora gli utenti finali dei nostri clienti attraverso le proprietà Internet.
- Cloudflare non profila gli utenti finali dei nostri clienti per vendere annunci pubblicitari.
- Cloudflare conserva i dati personali solo se necessario per fornire le soluzioni Cloudflare ai nostri clienti.

- Cloudflare non ha mai fornito a terzi o governi le chiavi di crittografia dei nostri clienti o un feed di contenuti dei clienti che transitano nella nostra rete e ci impegniamo da tempo a esaurire tutti i rimedi legali prima di soddisfare tale richiesta.
- Cloudflare si è pubblicamente impegnata a perseguire rimedi legali per contestare qualsiasi richiesta del governo degli Stati Uniti di dati che identifichiamo come soggetti al GDPR.
- La politica di Cloudflare consiste nel notificare ai nostri clienti qualsiasi procedimento legale che richieda le loro informazioni prima della loro possibile divulgazione, a meno che non sia legalmente vietato.

Certificazioni di sicurezza globali ed europee di Cloudflare

Cloudflare soddisfa gli standard leader di settore in termini di sicurezza e privacy e convalida tali impegni con revisori di terzi su base annuale.

Cloudflare è stata certificata secondo un nuovo standard internazionale sulla privacy per la protezione e la gestione del trattamento dei dati personali: ISO/IEC 27701:2019. Questo standard ha meno di due anni e adatta il concetto esistente di sistema di gestione della sicurezza delle informazioni nella creazione di un sistema di gestione delle informazioni sulla privacy (PIMS, Privacy Information Management System). Esistono requisiti per garantire che questo sistema di gestione della privacy sia solido e che venga costantemente migliorato per raggiungere gli obiettivi definiti. Lo standard è progettato in modo tale che i requisiti che le organizzazioni devono soddisfare per conseguire la certificazione siano strettamente allineati a quelli del GDPR.

In altre parole, la certificazione ISO 27701 garantisce ai nostri clienti che abbiamo un programma sulla privacy che è stato valutato da un soggetto esterno per soddisfare uno standard di settore internazionale allineato al GDPR e che ci impone di mantenere il nostro programma sulla privacy costantemente conforme. Questa certificazione, oltre al Data Processing Addendum (DPA) che mettiamo a disposizione dei nostri clienti nella dashboard, offre ai nostri clienti più

livelli di garanzia sul fatto che tutti i dati personali trattati da Cloudflare verranno gestiti in modo da soddisfare i requisiti del GDPR.

Inoltre, Cloudflare è conforme a [ISO 27001/27002](#), [Payment Card Industry Data Security Standards](#) (PCI DSS) e [SSAE 18 SOC 2 Type II](#). Queste convalide forniscono garanzie alle organizzazioni che trasferiscono i loro dati più sensibili attraverso i nostri servizi e contribuiscono inoltre a soddisfare e mantenere i propri obblighi di conformità.

Oltre alle regolari valutazioni di terzi rispetto agli standard del settore, Cloudflare è considerata un "operatore di servizi essenziali" ai sensi della direttiva dell'UE sulla sicurezza delle reti e dei sistemi informativi (direttiva NIS). Oltre a registrarsi ai sensi di questa direttiva con ICO e Ofcom nel Regno Unito, BSI in Germania e CNCS in Portogallo, Cloudflare è stata anche valutata rispetto a requisiti locali specifici, come il BSI Act in Germania (BSIG). Teniamo molto alle nostre relazioni e collaboriamo a stretto contatto con le autorità di regolamentazione locali europee sulla conformità e forniamo insight sulle nostre prassi di conformità ai requisiti di protezione dei dati.

A livello pratico, il GDPR era una codificazione di molte delle misure che avevamo già adottato:

- Cloudflare raccoglie solo i dati personali di cui ha bisogno per fornire il servizio offerto
- Cloudflare non vende informazioni personali
- Cloudflare offre alle persone la possibilità di accedere, correggere o eliminare le proprie informazioni personali
- Coerentemente con il suo ruolo di responsabile del trattamento dei dati, Cloudflare offre ai clienti il controllo sulle informazioni che, ad esempio, vengono memorizzate nella cache della sua rete di distribuzione dei contenuti (CDN, Content Delivery Network), archiviate nel Workers Key Value Store o acquisite dal suo Web Application Firewall (WAF)

Per saperne di più sul nostro impegno per il GDPR, visita: <https://www.cloudflare.com/it-it/trust-hub/gdpr/>.

Poiché ci teniamo alla protezione dei dati, non ci limitiamo a verificare dove siamo tenuti a farlo per legge o dove sono disponibili certificazioni. Il nostro team di sicurezza esegue rigorosi test di penetrazione interni ed esterni, gestiamo un programma di bug bounty tramite HackerOne e disponiamo di revisori di terzi per convalidare i nostri impegni sulla privacy. Gli esempi includono i nostri audit incentrati sulla privacy, come quello che abbiamo [condotto in relazione ai nostri impegni per il nostro resolver DNS pubblico 1.1.1.1](#). Siamo sempre disponibili a conseguire ulteriori convalide che forniranno garanzie nel nostro programma sulla privacy, nelle politiche e nelle prassi per il trattamento e la conservazione dei dati personali dell'UE.

I dati trattati da Cloudflare

Cloudflare tratta i dati dei registri degli utenti finali dei nostri clienti quando tali utenti finali accedono ai nostri servizi in linea con l'autorizzazione dei nostri clienti. Questi dati dei registri possono includere, a titolo esemplificativo, indirizzi IP, informazioni sulla configurazione del sistema e altre informazioni sul traffico da e verso i siti Web, i dispositivi, le applicazioni e/o le reti dei nostri clienti. Inoltre, Cloudflare raccoglie e archivia i dati e i registri delle attività del server e della rete durante l'utilizzo dei nostri prodotti ed effettua osservazioni e analisi dei dati sul traffico. La nostra [Informativa sulla privacy](#) descrive in modo più specifico le informazioni che raccogliamo e il modo in cui le utilizziamo.

Quando raccogliamo e archiviamo i dati delle attività sulla nostra rete, lo facciamo solo per migliorare i nostri prodotti per te, per gli altri nostri clienti o per la più ampia community di Internet. Non cerchiamo di monetizzare questi dati in alcun modo che pensiamo possa farti insorgere timori al riguardo. Ad esempio, possiamo archiviare e analizzare temporaneamente i dati sul traffico di rete di tutti i nostri clienti globali per instradare in modo intelligente le richieste attraverso i percorsi Internet più efficienti. Possiamo anche archiviare e analizzare i dati di rete per rilevare e identificare i vettori di minaccia emergenti che possiamo utilizzare immediatamente per migliorare i nostri strumenti di sicurezza. Infine, possiamo aggregare i dati di rete da segmenti di clienti significativamente ampi (ma mai da utenti o clienti identificabili individualmente) per aiutare la community di Internet a comprendere le tendenze e le minacce su Internet (vedi [Cloudflare Radar](#)).



I meccanismi di trasferimento dei dati di Cloudflare

Nel caso in cui Cloudflare, in qualità di responsabile del trattamento dei dati, trasferisca dati personali al di fuori dell'UE, lo fa in base al nostro Data Processing Agreement (DPA) standard, integrato nel nostro Contratto di servizio Enterprise e nel nostro Contratto di abbonamento self-service. Il nostro DPA contiene le clausole contrattuali standard dell'UE (SCC) (aggiornate nel 2021) per i dati soggetti al GDPR. Nel loro insieme, i termini di Cloudflare garantiscono un livello di protezione dei dati personali equivalente a quello garantito dal GDPR. Puoi trovare maggiori informazioni sul nostro impegno nei confronti del GDPR e sul nostro DPA [qui](#).

Secondo la decisione Schrems II, le SCC approvate dall'UE rimangono un meccanismo di trasferimento valido ai sensi del GDPR, in cui sono in vigore anche ulteriori salvaguardie per i dati trasferiti negli Stati Uniti. Cloudflare continuerà a utilizzare il meccanismo SCC per il trasferimento dei dati e ha aggiornato il nostro DPA standard per i clienti al fine di integrare ulteriori salvaguardie come impegni contrattuali. Ad esempio, ci impegniamo a perseguire rimedi legali per contestare qualsiasi richiesta del governo degli Stati Uniti di dati che identifichiamo come soggetti al GDPR e ci impegniamo a notificare ai nostri clienti qualsiasi procedimento legale che richieda le loro informazioni prima della divulgazione di queste, a meno che non sia legalmente vietato. Puoi visualizzare le garanzie aggiuntive che abbiamo aggiunto come impegni contrattuali nella sezione 7 del nostro [DPA](#).

Le normative e le linee guida sulla protezione dei dati sono in continua evoluzione e monitoriamo attentamente il panorama normativo e legislativo. Rivolgiamo continuamente uno sguardo al futuro delle linee guida emergenti per garantire che i nostri clienti e partner possano continuare a fruire dei vantaggi di Cloudflare in tutta Europa.

Per i clienti che devono assicurarsi che Cloudflare non stia trasferendo dati personali, offriamo una serie di misure tecniche note come Data Localization Suite.

Prodotti Cloudflare con funzionalità progettate per il supporto della localizzazione dei dati

Cloudflare si impegna ad aiutare i nostri clienti a mantenere i dati personali nell'UE. Offriamo una Data Localization Suite, che offre ai clienti il controllo su dove i loro dati vengono ispezionati e archiviati.

La nostra Data Localization Suite è composta da tre elementi:

1. Gestione delle chiavi di crittografia (Geo Key Manager e Keyless SSL)
2. Limite di ispezione dei payload (Regional Services)
3. Limite dei metadati del cliente

Gestione delle chiavi di crittografia:

La privacy dei dati non è possibile senza la sicurezza di Internet, fornita in gran parte da una crittografia efficace.

La crittografia dei dati trasmessi su una rete richiede l'uso di chiavi di crittografia, o set di valori matematici che sia il mittente che il destinatario di un messaggio crittografato conoscono. SSL/ TLS, un protocollo crittografico che rende possibile la comunicazione crittografata, utilizza una coppia di chiavi: una chiave pubblica e una chiave privata. I clienti di Cloudflare possono scegliere di utilizzare due funzionalità per garantire che le loro chiavi private non lascino l'UE:

- [Keyless SSL](#) consente ai clienti di archiviare e gestire le proprie chiavi private da utilizzare con Cloudflare. I clienti possono utilizzare un'ampia gamma di sistemi per il loro keystore, inclusi moduli di sicurezza hardware (HSM, Hardware Security Module), server virtuali e hardware in cui viene eseguito Unix/Linux e Windows ospitato in ambienti controllati dal cliente. Keyless SSL è keyless solo dal punto di vista di Cloudflare: Cloudflare non vede mai la chiave privata del cliente, ma il cliente la possiede e la utilizza. Nel frattempo, la chiave pubblica viene comunque utilizzata sul lato client come di consueto.
- [Geo Key Manager](#) offre ai clienti un controllo granulare sui datacenter in cui sono archiviate le loro chiavi private. Ad esempio, un cliente può scegliere che le chiavi private siano accessibili solo all'interno di datacenter situati nell'UE. Questo approccio libera i clienti dalla complessità della distribuzione di Keyless SSL e della manutenzione del proprio keystore.

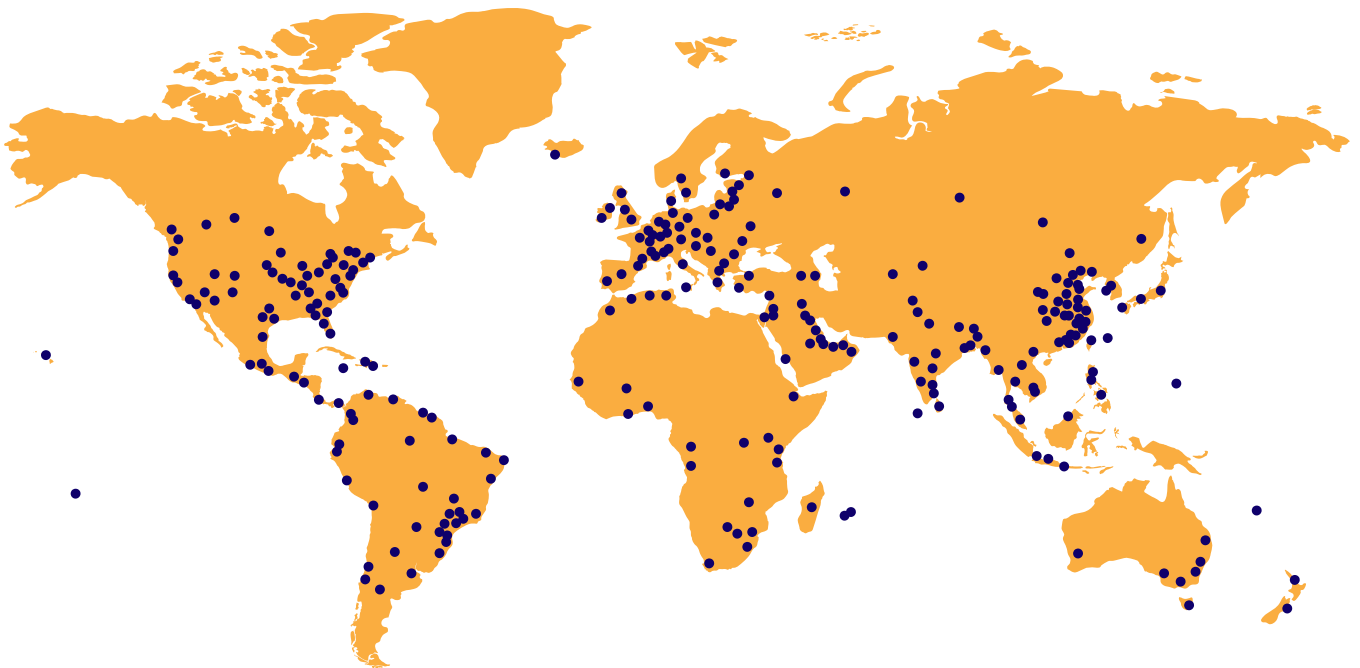
Limite dei metadati del cliente

Cloudflare offre i prodotti network-as-a-service più sicuri e con le prestazioni più elevate perché invia tramite proxy tutto il tuo traffico dal perimetro della nostra rete. In qualità di proxy autorizzato del tuo traffico, i nostri servizi ispezionano in modo sicuro il tuo traffico per identificare le minacce alla sicurezza e instradarlo da qualsiasi luogo attraverso la nostra rete globale. Cloudflare è uno dei pochi fornitori di servizi cloud progettato come una piattaforma globale unificata che può essere configurata anche per soddisfare requisiti locali specifici. Questa architettura offre ai clienti Cloudflare il controllo completo su dove e come viene ispezionato il traffico.

[Regional Services](#) di Cloudflare consente ai clienti di scegliere dove terminare le loro connessioni TLS nella rete Cloudflare. Ad esempio, un cliente potrebbe scegliere di far terminare tali connessioni nell'UE, quindi la decrittografia e l'ispezione dei contenuti del traffico HTTP avvengono solo all'interno dell'UE. Questa restrizione si applica a tutti i nostri servizi applicativi perimetrali, tra cui:

- Archiviazione e recupero di contenuti dalla cache
- Blocco dei payload HTTP dannosi con Web Application Firewall (WAF)
- Rilevamento e blocco di attività sospette con Bot Management
- Esecuzione di script Workers

Un caso d'uso ipotetico è quello di un cliente di Cloudflare in Germania che consente ai servizi locali di limitare la gestione all'UE. I clienti degli utenti finali si collegheranno alla località di Cloudflare più vicina in qualsiasi parte del mondo, ma se tale posizione si trova al di fuori dell'UE, il traffico viene trasferito a una località di Cloudflare nell'UE prima di essere ispezionato. Il cliente continua a beneficiare della nostra rete globale, a bassa latenza e ad alto throughput, in grado di resistere anche ai [più grandi attacchi DDoS](#). Tuttavia, Regional Services offre ai clienti anche controllo locale. Solo i datacenter all'interno dell'UE avranno l'accesso necessario per applicare le policy di sicurezza. Questo approccio consente a Cloudflare di selezionare il percorso più veloce verso l'UE e il punto di presenza disponibile più vicino per l'elaborazione.



Limite di ispezione dei payload

Il limite dei metadati del cliente di Cloudflare mantiene all'interno dell'UE i metadati del traffico degli utenti finali che possono identificare un cliente.

"Metadati" può essere un termine dal suono allarmante, ma è un concetto semplice: significa semplicemente "dati sui dati". In altre parole, è una descrizione delle attività avvenute sulla nostra rete. Ogni servizio su Internet raccoglie metadati in qualche forma ed è fondamentale per la sicurezza degli utenti e la disponibilità della rete.

La rete di Cloudflare è composta da decine di servizi: Firewall, Cache, resolver DNS, sistemi di protezione attacchi DDoS, Workers e altro ancora. Ogni servizio emette messaggi di registro strutturati, che contengono campi come indicazioni di data/ora, URL, utilizzo delle funzionalità di Cloudflare e l'identificativo dell'account e della zona del cliente.

Cloudflare utilizza i metadati sull'utilizzo dei nostri prodotti per diversi scopi:

- **Fornire analisi** tramite i nostri dashboard e API
- **Condividere registri** con i clienti
- **Bloccare le minacce alla sicurezza** come bot o attacchi DDoS
- **Migliorare le prestazioni** della nostra rete
- **Mantenere l'affidabilità** e la resilienza della nostra rete

Poiché i metadati non includono i contenuti del traffico dei clienti, non contengono nomi utente, password, informazioni personali e altri dettagli riservati degli utenti finali dei clienti. Tuttavia, i registri di servizio possono contenere indirizzi IP degli utenti finali, che sono considerati dati personali nell'UE.

Quando il limite dei metadati è abilitato per un cliente, il nostro perimetro garantisce che qualsiasi messaggio di registro che identifichi tale cliente (ovvero, contiene l'ID account di tale cliente) non venga inviato al di fuori dell'UE. Verrà inviato solo al nostro datacenter principale nell'UE e non al nostro datacenter negli Stati Uniti.

Quasi tutti i metadati degli utenti finali sono coperti dal limite dei metadati del cliente. Ciò include tutti i dati degli utenti finali per i quali Cloudflare è responsabile del trattamento, come definito nell'[Informativa sulla privacy di Cloudflare](#), per i servizi coperti. [Consulta qui](#) l'elenco più aggiornato dei tipi di dati e dei servizi Cloudflare coperti dal limite dei metadati del cliente.

Opportunità e responsabilità condivise

Poiché sappiamo che tutte le organizzazioni europee devono integrare i principi di privacy e sicurezza in ogni aspetto della loro attività, abbiamo preparato questo grafico per comprendere meglio chi è responsabile di questi requisiti di privacy comunemente richiesti:

Requisiti sulla privacy		
Principale	Responsabilità	Dettagli sulla responsabilità
Protezione dei dati fin dall'ideazione	Condivisa	<ul style="list-style-type: none">• Cloudflare è responsabile della fornitura di prodotti e servizi tenendo conto della privacy. Il team sulla privacy fornisce revisioni, valutazioni e formazione per garantire che la privacy sia instillata nel modo in cui lavoriamo.• I clienti sono responsabili dell'utilizzo e della configurazione dei propri servizi Cloudflare e devono rivedere periodicamente l'uso e la configurazione di questi servizi per convalidare che i principi di protezione dei dati siano stati considerati nella progettazione e nell'implementazione.
Richiesta di accesso degli interessati	Condivisa	<ul style="list-style-type: none">• Cloudflare fornisce agli interessati il diritto di accesso, correzione ed eliminazione delle informazioni personali indipendentemente dalla loro giurisdizione di residenza. Le richieste degli interessati possono essere inviate a sar@cloudflare.com.• Se riceviamo una richiesta da qualcuno che sembra essere un utente finale di uno dei nostri clienti, indirizzeremo tale persona a contattare direttamente il nostro cliente.

Requisiti sulla privacy		
Principale	Responsabilità	Dettagli sulla responsabilità
Sicurezza adeguata	Condivisa	<ul style="list-style-type: none"> • Cloudflare mantiene un programma di sicurezza in conformità con gli standard del settore. Il programma di sicurezza include il mantenimento di policy e procedure di sicurezza formali, la definizione di adeguati controlli degli accessi logici e materiali, nonché l'implementazione di salvaguardie tecniche negli ambienti aziendali e di produzione, tra cui la creazione di configurazioni sicure, trasmissione e connessioni protette, registrazione, monitoraggio e tecnologie adeguate per la crittografia dei dati personali. • I clienti sono responsabili della revisione dello stato di sicurezza dei loro fornitore di servizi cloud come Cloudflare e possono farlo esaminando le nostre convalide e i nostri report di conformità. Esortiamo inoltre i nostri clienti a rivedere le impostazioni di sicurezza del dashboard per garantire che aderiscano alle loro policy e procedure di sicurezza.
Base giuridica per il trattamento	Condivisa	<ul style="list-style-type: none"> • Cloudflare tratta i dati secondo le istruzioni dei nostri clienti, i titolari del trattamento dei dati, e opera come responsabile del trattamento dei dati in conformità con il GDPR. • I clienti hanno la responsabilità di garantire di disporre di una base giuridica adeguata per il trattamento dei dati dei propri utenti finali.
Violazioni dei dati personali	Condivisa	<ul style="list-style-type: none"> • Cloudflare informerà i clienti non appena viene a conoscenza di qualsiasi violazione della sicurezza che causi la perdita, la divulgazione non autorizzata o l'accesso ai dati personali trattati da Cloudflare o dai suoi responsabili secondari. Cloudflare è inoltre responsabile di fornire ai nostri clienti ragionevole cooperazione e assistenza alla luce della violazione, inclusa la fornitura ai clienti di informazioni ragionevoli in possesso di Cloudflare in merito alle circostanze della violazione e ai dati personali interessati. • I clienti sono responsabili del rispetto dei requisiti normativi o contrattuali per notificare ai propri utenti finali e/o alle autorità governative qualsiasi violazione dei dati personali.

Una rete cloud globale basata sulla fiducia dei clienti

La prima priorità di Cloudflare è guadagnare e mantenere la fiducia dei clienti. Comprendiamo che la trasparenza negli impegni di Cloudflare sulla privacy e nel nostro approccio per l'integrazione della località dei dati e delle salvaguardie della privacy nella nostra rete e nei nostri prodotti aiuti i clienti a soddisfare i propri obblighi. Comprendiamo anche che le certificazioni di settore e i meccanismi di contrattazione ben progettati di Cloudflare ci aiutino a creare un solido rapporto di fiducia con i nostri clienti europei. I team di privacy e sicurezza di Cloudflare sono qui per collaborare con te per soddisfare i requisiti più rigorosi che potresti dover affrontare nel tuo paese, area geografica o settore. I nostri Account Executive, Customer Success Manager e Sales Engineer esperti collaborano regolarmente con i nostri team di conformità alla privacy e alla sicurezza per aiutare i nostri clienti a configurare i prodotti Cloudflare che utilizzano per soddisfare i loro specifici obblighi di conformità. Se desideri una dimostrazione o una sessione specializzata sulla configurazione dei tuoi servizi per soddisfare i tuoi obblighi specifici, contattaci oggi stesso. Inviaci un'e-mail all'indirizzo privacyquestions@cloudflare.com o security@cloudflare.com.





Il presente documento ha finalità puramente divulgative ed è di proprietà di Cloudflare. Il presente documento non comporta alcun impegno o garanzia da parte di Cloudflare o delle sue affiliate nei confronti dell'utente. È responsabilità dell'utente valutare in modo autonomo le informazioni contenute nel presente documento. Le informazioni contenute nel presente documento sono soggette a modifiche e non si intendono esaurienti né riportano tutte le indicazioni di cui l'utente potrebbe avere bisogno. Le responsabilità e gli obblighi di Cloudflare nei confronti dei suoi clienti sono disciplinati da accordi specifici e il presente documento non integra né modifica alcun accordo tra Cloudflare e i suoi clienti. I servizi di Cloudflare vengono erogati "così come sono" senza garanzie, dichiarazioni o condizioni di alcun tipo, sia espresse che implicite.

© 2024 Cloudflare, Inc. Tutti i diritti riservati. CLOUDFLARE® e il logo Cloudflare sono marchi di Cloudflare. Tutti gli altri nomi e i loghi di società e prodotti possono essere marchi delle società cui sono rispettivamente associati.