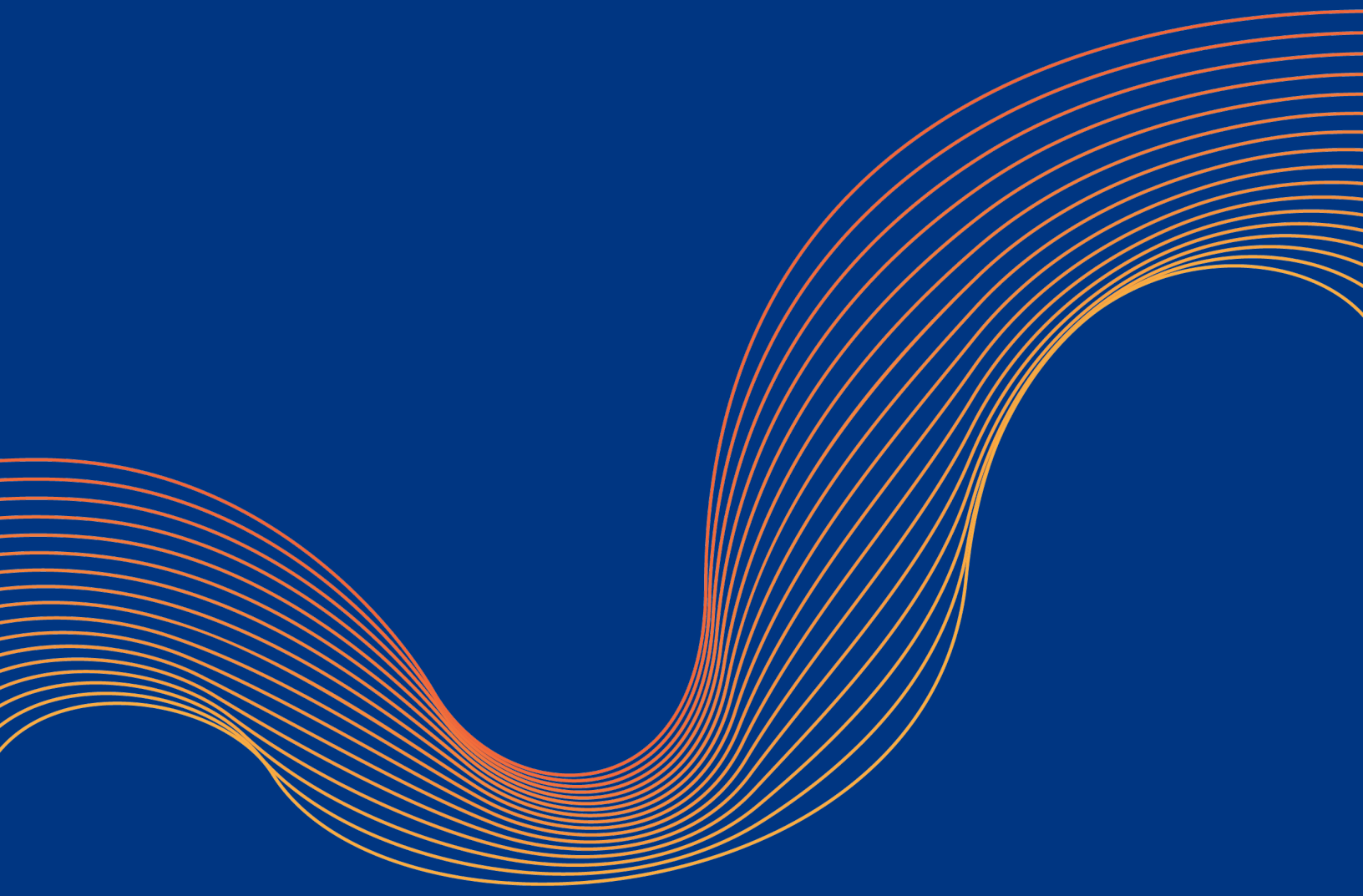
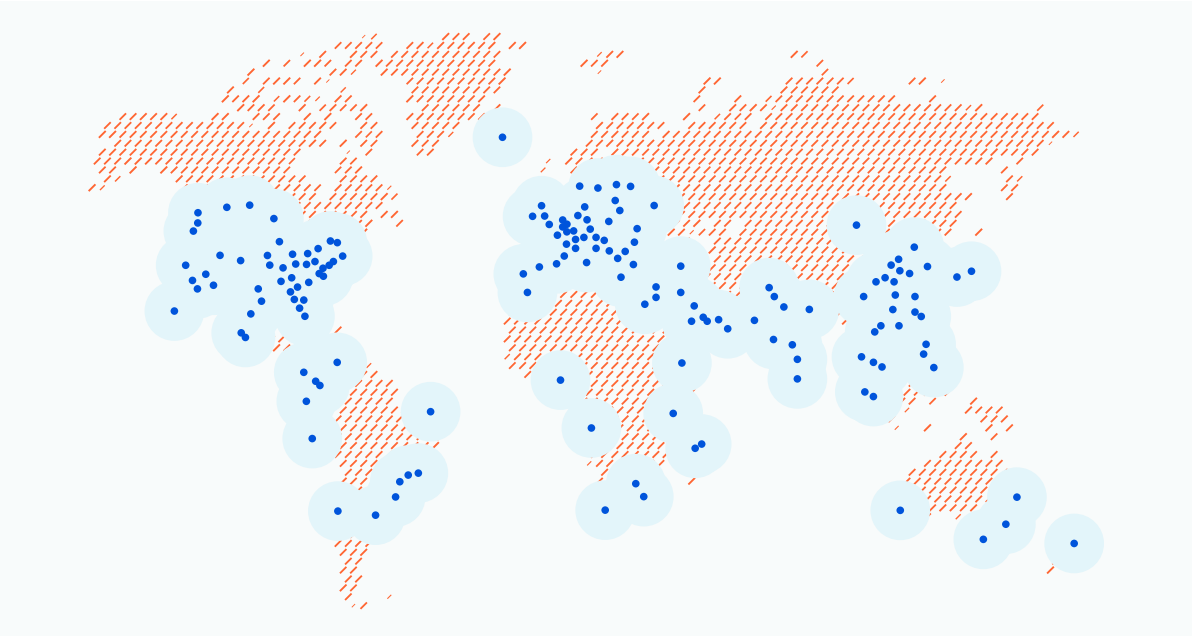
WHITEPAPER

CLOUDFLARE

Come Cloudflare aiuta a rispettare il principio di località e gli obblighi di riservatezza in Europa



1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com



La sofisticata rete cloud globale di Cloudflare dispone di oltre 200 punti di presenza fisica sparsi in più di 100 Paesi. Cloudflare fornisce agli utenti gli strumenti necessari per gestire il modo in cui i dati sensibili vengono instradati tra questi datacenter, consentendo loro di personalizzare il traffico per soddisfare le loro esigenze in termini di sicurezza, privacy e prestazioni.

Cloudflare e la fiducia dei clienti

La missione di Cloudflare è aiutare a creare un Internet migliore. Abbiamo una piattaforma cloud globale che offre un'ampia gamma di servizi di rete a persone fisiche e aziende di ogni dimensione in tutto il mondo. La rete Cloudflare e il suo portfolio in continua espansione migliorano la sicurezza, le prestazioni e l'affidabilità di tutto ciò che viene connesso a Internet. Oltre a servire i propri clienti, Cloudflare si propone inoltre di migliorare la stessa rete Internet rendendola sempre attiva, sempre veloce, sempre sicura, sempre riservata e disponibile per tutti.

La rete Cloudflare, la sua community di sviluppatori e il suo business dipendono totalmente dalla fiducia dei clienti. Cerchiamo costantemente di conquistare e consolidare la fiducia dei clienti comportandoci in modo trasparente rispetto ai nostri obblighi in materia di privacy e al modo in cui trattiamo i dati di clienti e utenti finali nei nostri sistemi. Alimentiamo la loro fiducia anche realizzando e implementando prodotti in grado di (i) migliorare la sicurezza dei nostri sistemi, (ii) crittografare i dati inattivi o in transito, e (iii) permettere ai nostri clienti di stabilire le modalità di controllo del traffico nelle differenti ubicazioni sparse nel mondo. Infine, generiamo la fiducia dei clienti ottenendo e rinnovando certificazioni del settore (ad esempio SSAE 18 SOC 2 Tipo II) ed elaborando meccanismi di contrattazione (come gli accordi sul trattamento dei dati) che definiscono il modello di responsabilità condivisa con i clienti per garantire la privacy.

Cloudflare in Europa

Oggi, Cloudflare è utilizzato da oltre 25 milioni di proprietà Internet in tutto il mondo. Questo elenco comprende molte delle più grandi e più dinamiche aziende europee, tra cui Eurovision, L'Oreal, AO.com, AllSaints e molti altri marchi famosi. Include anche una serie sempre più lunga di importanti istituzioni europee, tra cui INSEAD, Börse Stuttgart, IATA e Great Rail Journeys. Essendo sempre più dipendenti da Internet come piattaforma cruciale per fornire servizi a clienti, utenti e diretti interessati, molte imprese e organizzazioni di vario tipo stanno adottando rapidamente reti cloud sicure e affidabili come Cloudflare per proteggere le applicazioni, le infrastrutture e le persone connesse a Internet da minacce di ogni genere.

La piattaforma Internet di Cloudflare è stata progettata per soddisfare i requisiti dei settori più attenti alla privacy e più regolamentati d'Europa, come il settore bancario, la pubblica amministrazione, l'industria energetica, il servizi pubblici, la vendita al dettaglio, il gioco online e la sanità. In Cloudflare realizziamo prodotti in grado di soddisfare i più elevati standard di sicurezza e privacy degli utenti, e collaboriamo a stretto contatto con i nostri clienti in Europa per aiutarli a rispettare gli obblighi in materia di protezione dei dati vigenti nei rispettivi Paesi e settori industriali.

Il forte impegno di Cloudflare a favore della privacy

Cloudflare è stata creata per aiutare i nostri utenti e i loro clienti a godere di una maggiore sicurezza su Internet. La nostra rete e tutti i nostri prodotti sono realizzati pensando alla protezione dei dati. Siamo innanzitutto una società che garantisce rigorosamente la tutela della privacy: come specificato nella nostra Informativa sulla privacy, ci impegniamo a non vendere i dati personali che trattiamo per conto dei nostri clienti e a non utilizzarli per scopi diversi da quello di prestare loro i nostri servizi. Nel corso della nostra storia non abbiamo mai tradito questa promessa. In effetti, il nostro approccio nei confronti della privacy è stato definito molto prima che i governi iniziassero a regolamentarla forzando molte altre aziende tecnologiche ad aggiornare le proprie policy per dare opportuno rilievo alla privacy di clienti e utenti. Non ricaviamo utili dalla pubblicità, ma solo dalla raccolta e dalla conservazione dei dati personali che trattiamo per conto dei nostri utenti.

In veste di responsabile del trattamento dei dati e di provider di servizi, Cloudflare elabora i dati dei log degli utenti per conto dei nostri clienti quando i loro utenti finali accedono ai nostri servizi su autorizzazione dei nostri clienti. I dati dei log elaborati possono comprendere, in forma non limitativa, indirizzi IP, informazioni sulla configurazione di sistemi e altre informazioni sul traffico in entrata e in uscita su siti web, dispositivi, applicazioni e/o reti dei nostri clienti. La nostra Informativa sulla privacy descrive le informazioni che raccogliamo e gli usi che ne facciamo. Inoltre, in veste di titolare del trattamento dei dati, Cloudflare raccoglie e conserva i dati e i log relativi all'attività di server e rete durante il funzionamento del Servizio e fornisce osservazioni e analisi dei dati sul traffico (chiamiamo questi dati "Metriche operative"). Tra gli esempi di Metriche operative vi sono quelle relative a uptime e disponibilità del servizio, volumi delle richieste, tassi di errore, tassi delle cache e valutazioni delle minacce IP.

Quando raccogliamo e archiviamo i dati delle attività sulla nostra rete, lo facciamo solo per rendere migliori i nostri prodotti per i nostri clienti o per tutta la community di Internet. Non cerchiamo di monetizzare questi dati in alcun modo che possa sorprendervi. Ad esempio, possiamo conservare temporaneamente e analizzare i dati del traffico di rete relativi ai nostri clienti a livello globale per poter instradare gli utenti finali in modo intelligente attraverso i percorsi meno congestionati e più affidabili di Internet. Possiamo conservare e analizzare i dati di rete anche per individuare e identificare eventuali vettori di minacce emergenti che possiamo impiegare immediatamente per aggiornare il modo in cui i nostri prodotti proteggono le proprietà Internet degli utenti. Inoltre, possiamo aggregare i dati di rete relativi a un numero significativo di clienti (ma in nessun caso di utenti o clienti individualmente identificabili) per aiutare la community di Internet a comprendere informazioni, minacce e tendenze presenti in Internet (vedere Cloudflare Radar). Infine, i dati di rete che raccogliamo e conserviamo sono utilizzati solamente per migliorare la nostra rete e i nostri prodotti per i nostri clienti, oppure per condividere le tendenze globali di Internet con tutti gli utenti di Internet.

Di seguito è possibile vedere alcuni dei nostri impegni in materia di privacy che ci differenziano da molti altri provider di servizi cloud:

- Cloudflare non vende i dati personali.
- Cloudflare non monitora gli utenti finali dei propri clienti attraverso le proprietà Internet.
- Cloudflare non effettua la profilazione degli utenti finali dei propri clienti per vendere annunci pubblicitari.
- Cloudflare conserva i dati personali solo per il tempo necessario per fornire le proprie offerte ai propri clienti.
- Cloudflare non ha mai fornito le chiavi di crittografia dei nostri clienti o parti del contenuto dei clienti in transito sulla nostra rete ad alcuna terza parte o governo, e ci impegniamo da molto tempo a ricorrere a tutti i mezzi legali prima di soddisfare questo genere di richieste.
- Cloudflare si è impegnata pubblicamente a ricorrere ai mezzi legali per opporsi a qualsiasi richiesta del governo degli Stati Uniti relativamente a dati che risultino essere soggetti al Regolamento generale sulla protezione dei dati RDGP.
- Prima di procedere alla divulgazione, la politica di Cloudflare prevede di informare i clienti di eventuali processi legali che richiedono le loro informazioni, tranne ove ciò sia vietato dalla legge.

Caratteristiche dei prodotti Cloudflare progettate per soddisfare i requisiti di protezione dei dati

I nostri clienti europei utilizzano spesso le seguenti funzionalità per configurare le proprie implementazioni di Cloudflare e soddisfare così gli obblighi legali in materia di trattamento dei dati:

Dashboard e sicurezza del portale:
La dashboard di Cloudflare mette a disposizione un'interfaccia utente facile da usare che permette ai clienti di configurare e gestire tutti i prodotti che usano e che sono in funzione sulla rete Cloudflare. I clienti si connettono alla Dashboard di Cloudflare tramite i portali web protetti di Cloudflare. Per aiutare i clienti a garantire un accesso protetto e autorizzato agli account e ai dati dei clienti di Cloudflare, abbiamo implementato funzioni di sicurezza standard nei nostri portali e nella nostra Dashboard. Abbiamo riscontrato che molte società e organizzazioni non riescono a garantire un accesso sicuro ai propri dispositivi, prodotti e servizi di sicurezza. I prodotti Cloudflare sono invece basati su un'unica piattaforma protetta, che offre ai clienti di Cloudflare un accesso costante ed estremamente sicuro agli account per tutti i prodotti che garantiscono sicurezza, prestazioni e affidabilità.

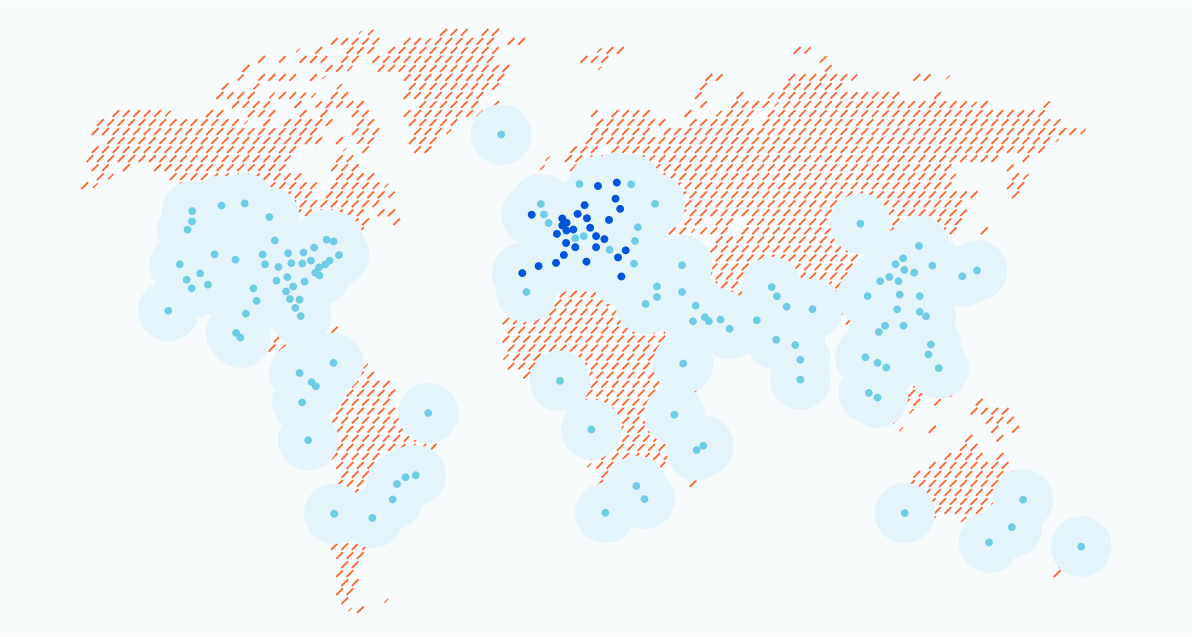
- **L'autenticazione a due fattori** (2FA) migliora la sicurezza degli account richiedendo un secondo gruppo di informazioni per convalidare l'identità dell'utente al momento del login. L'autenticazione 2FA di Cloudflare supporta i token hardware e le app per dispositivi mobili TOTP.
- **Le funzioni Accesso Unico** (se abilitate) consentono ai clienti di utilizzare un provider di identità in loco o ospitato sul cloud per il controllo degli accessi. Fare clic qui per vedere l'elenco completo dei provider supportati.
- **I log di controllo** riepilogano la cronologia degli accessi e delle modifiche apportate alla configurazione Cloudflare di un cliente. I log di controllo comprendono azioni a livello di account come login e logout, oltre a modifiche alle impostazioni relative a funzioni come DNS, Crypto, Firewall, Speed, Caching, Page Rules, Network e Traffic, ecc. I log di controllo sono disponibili su tutti i tipi di piani e vengono registrati sia per i singoli utenti che per le organizzazioni multiutente.

Crittografia:
La crittografia è un modo di criptare i dati che consente solo alle parti autorizzate di comprendere le informazioni. I dati possono essere crittografati quando sono "inattivi", vale a dire quando sono archiviati, o "in transito", vale a dire mentre vengono trasmessi altrove. La crittografia dei dati trasmessi su una rete richiede l'uso di una chiave di crittografia: un gruppo di valori matematici noti sia al mittente, sia al destinatario di un messaggio crittografato.

La crittografia impedisce alle parti non autorizzate, siano esse utenti malintenzionati, reti pubblicitarie, provider di servizi Internet o elementi ostili esterni, di intercettare e leggere i dati sensibili. Le comunicazioni crittografate consentono alle parti che comunicano di scambiare dati sensibili senza rischiare di perderli. La crittografia aiuta anche a impedire eventuali comportamenti dannosi come gli attacchi "on-path". Molte normative di settore e dei governi richiedono alle società che gestiscono i dati degli utenti di conservarli in forma crittografata. Tra gli esempi di standard normativi e di conformità che richiedono l'uso della crittografia vi sono HIPAA, PCI-DSS e RGPD.

Cloudflare offre i prodotti Network-as-as-Service più sicuri e dalle migliori prestazioni, poiché inoltriamo tutto il traffico dei nostri utenti direttamente dal perimetro della nostra rete. In veste di proxy autorizzato per il traffico dei nostri utenti, esaminiamo accuratamente il traffico per rilevare eventuali minacce alla sicurezza e lo gestiamo da qualsiasi ubicazione per incanalarlo lungo la nostra rete globale. Cloudflare offre agli utenti la possibilità di determinare dove e come il traffico viene controllato. Cloudflare è uno dei pochi cloud provider concepiti come una piattaforma globale unificata che può essere configurata per soddisfare specifici requisiti locali.

Servizi Regionali consente alle organizzazioni di verificare dove il loro traffico viene controllato. Con Servizi Regionali abilitato, il traffico viene inserito nella Anycast network globale di Cloudflare nella posizione più vicina al cliente. Invece di essere controllato in quel punto di presenza (PoP), il traffico viene instradato in modo protetto verso i PoP di Cloudflare situati nelle regioni selezionate dal cliente, dove viene quindi elaborato. Se viene applicato anche Geo Key Manager, le chiavi TLS del cliente vengono archiviate e utilizzate solo per gestire il traffico all'interno di quelle regioni. Servizi Regionali aiuta i clienti che desiderano mantenere il controllo locale sul proprio traffico mantenendo al contempo i vantaggi in termini di sicurezza offerti da una rete globale.



Ad esempio, un cliente Cloudflare in Germania può abilitare Servizi Regionali per limitare l'elaborazione all'UE. I suoi utenti finali si connetteranno alla sede Cloudflare più vicina ovunque nel mondo ma, se tale ubicazione è fuori dall'UE, prima di essere esaminato il traffico sarà passato a una sede Cloudflare in UE. Il cliente può usufruire comunque dei benefici della nostra rete globale a bassa latenza ed elevato throughput, la quale è in grado di sopportare anche i più grandi attacchi DDoS. Tuttavia, Servizi Regionali assicura ai clienti anche il controllo locale; solo i datacenter all'interno dell'UE disporranno dell'accesso necessario per applicare le politiche di sicurezza. Questo approccio permette a Cloudflare di selezionare il percorso più veloce verso l'UE e il punto di presenza più vicino disponibile per l'elaborazione.

Oltre a specificare il punto in cui il traffico deve essere controllato, Cloudflare aiuta le società a proteggere utenti e dati utilizzando le più avanzate tecniche e tecnologie di crittografia del settore. Geo Key Manager e Keyless SSL assicurano ai clienti il completo controllo sulle posizioni in cui le chiavi vengono archiviate e sui PoP che vi hanno accesso.

Keyless SSL consente ai clienti di archiviare e gestire le proprie chiavi private SSL da utilizzare con Cloudflare. I clienti possono utilizzare un'ampia gamma di sistemi per il loro keystore, tra cui moduli di sicurezza hardware ("HSM"), server virtuali e hardware con Unix/Linux e Windows ospitati in ambienti controllati dai clienti. Keyless SSL impiega vari metodi per creare una connessione protetta per la trasmissione delle chiavi dal cliente a Cloudflare, e assicura la persistenza della sessione che in genere accelera la velocità generale della transazione SSL.

Geo Key Manager fornisce ai clienti un controllo preciso sull'ubicazione in cui sono archiviate le loro chiavi. Ad esempio, un cliente può scegliere che le proprie chiavi private possano essere accessibili solo all'interno dei PoP ubicati nell'UE.

Con Cloudflare, i clienti dispongono di un controllo capillare non solo sull'ubicazione in cui vengono archiviate le loro chiavi private, ma anche sulla posizione in cui il traffico viene effettivamente ispezionato per verificare l'assenza di minacce per la sicurezza. Se un cliente lo desidera, il traffico può essere esaminato solo in PoP ubicati negli stati membri dell'UE.

Certificazioni di sicurezza globali ed europee di Cloudflare

Cloudflare rispetta i principali standard del settore in materia di sicurezza e privacy, e convalida queste certificazioni su base annuale tramite revisori di terze parti. Cloudflare è conforme alle normative ISO 27001/27002, Payment Card Industry Data Security Standards (PCI DSS) e SSAE 18SOC 2 Tipo II. Abbiamo firmato accordi con partner commerciali e siamo in grado di soddisfare i requisiti delle aziende in conformità all'Health Insurance Portability and Accountability Act del 1996 (HIPAA). Queste validazioni garantiscono le organizzazioni che trasferiscono i propri dati più sensibili attraverso i nostri servizi, oltre ad aiutarle a rispettare e assumersi gli obblighi di conformità.

In aggiunta alle regolari valutazioni di terze parti rispetto agli standard di 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 sotto questa direttiva presso ICO e Ofcom nel Regno Unito, BSI in Germania e CNCS in Portogallo, Cloudflare è anche stata valutata rispetto a specifici requisiti regionali, ad esempio il BSI Act in Germania (BSIG). Abbiamo relazioni di lavoro e collaboriamo strettamente con gli enti regolatori europei in materia di conformità, e forniamo informazioni dettagliate su come soddisfiamo i requisiti in materia di protezione dei dati.

A livello pratico, l'apposito Regolamento generale sulla protezione dei dati (RGPD) europeo ha codificato molte delle prassi da noi già adottate:

- Cloudflare raccoglie solamente i dati personali necessari per fornire il servizio che offriamo
- Cloudflare non vende informazioni personali
- Cloudflare dà alle persone la possibilità di accedere, correggere o eliminare le proprie informazioni personali
- Coerentemente con il nostro ruolo di responsabile del trattamento dei dati, Cloudflare concede ai clienti il controllo sulle informazioni che, ad esempio, sono inserite nella cache sulla nostra Content Delivery Network (CDN), archiviate in Workers Key Value Store o acquisite dal nostro Web Application Firewall (WAF)

Le domande frequenti sul nostro RGPD possono essere consultate all'indirizzo cloudflare.com/gdpr/introduction.

Data la nostra attenzione alla protezione dei dati, non ci limitiamo a esaminarli dove siamo tenuti a farlo per legge o dove sono disponibili le certificazioni. Il team addetto alla sicurezza esegue rigorosi test di penetrazione interni ed esterni, portiamo avanti un programma "premio a chi trova l'errore" tramite HackerOne e impieghiamo revisori di terze parti per convalidare i nostri impegni a favore della privacy. Esempi importanti in materia sono i controlli incentrati sulla privacy, come quello che abbiamo condotto all'inizio di quest'anno sui nostri impegni per il nostro resolver DNS pubblico 1.1.1.1. Siamo sempre pronti a ottenere ulteriori convalide in grado di fornire garanzie sui nostri programmi, le nostre politiche e le nostre pratiche in materia di privacy per il trattamento e l'archiviazione dei dati personali nell'UE.

Meccanismi di trasferimento dei dati di Cloudflare

I tipi di dati personali elaborati da Cloudflare per conto di un cliente dipendono da quali servizi di Cloudflare vengono implementati. La maggior parte dei dati che transitano sulla rete Cloudflare rimangono sui suoi server perimetrali, mentre i dati dei log relativi a questa attività possono essere elaborati per conto dei nostri clienti nel nostro datacenter core negli Stati Uniti, anche quando i clienti abilitano Servizi Regionali.

Alcuni dati di questi log comprenderanno informazioni sui visitatori e gli utenti autorizzati di domini, reti, siti web, interfacce per programmi applicativi ("API") o applicazioni dei nostri clienti. Questi metadati contengono dati personali estremamente limitati, in maggioranza sotto forma di indirizzi IP. Elaboriamo questo tipo di informazioni per conto dei nostri clienti nel nostro datacenter core negli Stati Uniti per un periodo di tempo limitato.

Dal momento che alcuni dati personali limitati vengono trasferiti negli Stati Uniti, abbiamo implementato un sistema che facilita alle aziende il compito di mantenere un meccanismo di trasferimento dei dati valido durante l'uso dei servizi di Cloudflare. Il nostro Accordo sul trattamento dei dati (DPA) standard è integrato nel nostro Contratto di servizio aziendale, e il DPA comprende le EU Clausole contrattuali standard (SCC) per i dati soggetti al RGPD. Presi insieme, i termini di Cloudflare assicurano un livello di protezione dei dati personali equivalente a quello garantito ai sensi del RGPD. Ulteriori informazioni sul nostro impegno a favore del RGPD e sul nostro DPA sono disponibili qui.

Il 16 luglio 2020, la Corte di giustizia dell'Unione Europea ("CGUE") ha preso una decisione che invalida il paradigma del Privacy Shield UE-USA nel caso "Schrems II". Di conseguenza, alcuni nostri clienti che elaborano i dati di residenti nell'UE ci hanno chiesto che cosa comporti questa decisione per la legalità dei trasferimenti negli Stati Uniti dei dati elaborati da Cloudflare per loro conto. Per prima cosa, l'invalidazione del Privacy Shield non modifica gli efficaci metodi di protezione della privacy dei dati implementati da Cloudflare per i dati personali che elaboriamo per conto dei nostri clienti; inoltre noi continueremo a seguire i principi di protezione dei dati che ci siamo impegnati a rispettare quando siamo stati certificati ai sensi del Privacy Shield.

Nell'ambito della decisione "Schrems II", le SCC approvate dall'UE rimangono un meccanismo di trasferimento valido ai sensi del RGPD laddove vengano adottate ulteriori salvaguardie per i dati trasferiti negli Stati Uniti. Cloudflare continuerà a utilizzare il meccanismo delle SCC per il trasferimento di dati, e abbiamo aggiornato il nostro DPA standard per clienti in modo da includere ulteriori salvaguardie previste come impegni contrattuali. Ad esempio, prima di divulgare informazioni degli utenti, ci impegniamo a impiegare ogni mezzo legale per opporci a eventuali richieste del governo degli Stati Uniti riguardanti dati da noi identificati come soggetti al RGPD, e ci impegniamo a informare i nostri clienti di eventuali processi legali che richiedano le loro informazioni, tranne ove vietato dalla legge. Le ulteriori salvaguardie aggiunte come impegni contrattuali possono essere consultate nella sezione 7 del nostro DPA.

Le normative e le linee guida sulla protezione dei dati sono soggette a una continua evoluzione e noi monitoriamo attentamente il panorama normativo e legislativo. Guardiamo continuamente avanti alla ricerca di nuove indicazioni per garantire che clienti e partner possano continuare a usufruire dei benefici di Cloudflare in Europa.

Opportunità e responsabilità condivise

Poiché sappiamo che tutte le organizzazioni europee devono integrare i principi relativi a privacy e sicurezza in ogni fase delle proprie attività, abbiamo preparato questa tabella per aiutare a comprendere chi sia responsabile di questi requisiti sulla privacy comunemente richiesti:

Principio	Responsabilità	Dettagli sulle responsabilità
Protezione dei dati in fase di progettazione	Condivisa	Cloudflare ha la responsabilità di fornire prodotti e servizi che tengano in considerazione la privacy. Il team addetto alla privacy fornisce revisioni, valutazioni e formazione per garantire che la privacy sia parte integrante del modo in cui lavoriamo. I clienti sono responsabili dell'uso e della configurazione dei propri servizi Cloudflare e devono rivedere periodicamente l'uso e la configurazione di questi servizi per verificare che i principi di protezione dei dati siano stati adeguatamente considerati durante la loro progettazione e implementazione.
Richiesta di accesso dell'interessato	Condivisa	Cloudflare dà agli interessati il diritto di accedere, correggere ed eliminare le informazioni personali, indipendentemente dalla loro giurisdizione di residenza. Le richieste degli interessati possono essere inviate all'indirizzo sar@cloudflare.com. Quando riceviamo una richiesta da qualcuno che sembra essere un utente finale di un nostro cliente, invitiamo la persona in questione a contattare direttamente il nostro cliente.

Principio	Responsabilità	Dettagli sulle responsabilità
Sicurezza adeguata	Condivisa	Cloudflare implementa un programma di sicurezza conforme agli standard di settore. Questo programma di sicurezza comprende lo sviluppo di politiche e procedure di sicurezza formali, la definizione di adeguati controlli degli accessi logici e fisici, l'implementazione di metodi di salvaguardia tecnica in ambienti aziendali e di produzione (compresa la definizione di configurazioni sicure, trasmissione e collegamenti protetti, creazione di log e monitoraggio) e la disponibilità di adeguate tecnologie di crittografia per i dati personali. I clienti hanno la responsabilità di rivedere lo stato di sicurezza dei cloud provider come Cloudflare, e possono farlo riesaminando le validazioni e i report di conformità. Incoraggiamo i nostri clienti anche a rivedere le impostazioni di sicurezza della propria Dashboard, per verificare che siano conformi alle loro politiche e procedure di sicurezza.
Base legale per l'elaborazione	Condivisa	Cloudflare elabora i dati in conformità alle istruzioni dei nostri clienti, i titolari del trattamento dei dati, e opera in veste di responsabile del trattamento dei dati conforme al RGPD. I clienti hanno la responsabilità di verificare di disporre di una base legale adeguata per l'elaborazione dei dati dei propri utenti finali.
Violazioni dei dati personali	Condivisa	Cloudflare informerà tempestivamente i clienti non appena sia venuta a conoscenza di eventuali violazioni della sicurezza che comportano perdita, diffusione non autorizzata o accesso a dati personali elaborati da Cloudflare o dai suoi co-responsabili. Cloudflare ha anche la responsabilità di garantire ai clienti un livello ragionevole di cooperazione e assistenza in caso di violazioni, ivi inclusa la fornitura ai clienti di informazioni appropriate in possesso di Cloudflare e riguardanti le circostanze della violazione e i dati personali interessati. I clienti hanno la responsabilità di rispettare i requisiti normativi o contrattuali, per segnalare eventuali violazioni dei dati personali ai danni dei propri utenti finali e/o delle autorità di un governo.

Una rete cloud globale costruita sulla fiducia dei clienti

La prima priorità di Cloudflare è conquistare e consolidare la fiducia dei clienti. Sappiamo che la trasparenza rispetto all'impegno in difesa della privacy assunto da Cloudflare e al metodo utilizzato per garantire la conformità ai principi di località e tutela della privacy nella nostra rete e nei nostri prodotti, aiuta i clienti a soddisfare i propri obblighi. Sappiamo anche che le certificazioni di settore e i ben congegnati meccanismi di contrattazione di Cloudflare ci aiutano a creare un solido rapporto di fiducia con i nostri clienti europei.

I team addetti alla privacy e alla sicurezza di Cloudflare sono qui per collaborare con i nostri utenti, al fine di soddisfare i più severi requisiti che gli utenti devono affrontare nel proprio Paese, nella propria regione o nel proprio settore. I nostri esperti Responsabile account, Responsabile successo del cliente e Ingegnere vendite collaborano regolarmente con i team responsabili della conformità in materia di privacy e sicurezza per aiutare i nostri clienti a configurare i prodotti Cloudflare che utilizzano per soddisfare i propri specifici obblighi in materia di conformità. Contattateci oggi stesso per chiedere una dimostrazione o una sessione specializzata sulla configurazione dei servizi per soddisfare specifici requisiti. Inviate un'e-mail agli indirizzi privacyquestions@cloudflare.com o security@cloudflare.com.

ULTERIORI INFORMAZIONI

1. **Informazioni sui servizi di registrazione di Cloudflare**
2. **Gestione e analisi dei log**
3. **Domande frequenti sui log**
4. **Contattateci** per abilitare Servizi Regionali