Dropbox

Protezione della privacy e dei dati

Introduzione

I dati personali giocano un ruolo enorme nella società e nell'economia. Sempre più spesso le persone chiedono maggiore controllo e chiarezza sul modo in cui i loro dati personali vengono utilizzati e protetti dalle organizzazioni con cui interagiscono. Allo stesso tempo, le persone prediligono organizzazioni con linee guida chiare in materia di tutela dei dati personali.

In Dropbox, la fiducia è alla base del nostro rapporto con milioni di persone e aziende in tutto il mondo. La fiducia che hai riposto in noi è molto importante e ci assumiamo la responsabilità di proteggere i tuoi dati personali con la massima serietà.

Il nostro impegno nei tuoi confronti

Ci impegniamo a proteggere i tuoi dati personali. I Termini di servizio di Dropbox definiscono le tue responsabilità quando utilizzi i nostri servizi. Le nostre Norme sulla privacy descrivono i nostri impegni alla privacy nei confronti degli utenti e spiegano come raccogliamo, utilizziamo e gestiamo i tuoi dati personali quando utilizzi i nostri servizi. Se risiedi nell'Unione Europea (UE), i tuoi dati personali sono controllati da Dropbox International Unlimited Company, che ha sede in Irlanda.

Se sei un utente Dropbox Business o Dropbox Education, la tua organizzazione agisce come responsabile del trattamento dei dati personali forniti a Dropbox in relazione all'uso di Dropbox Business o Dropbox Education. Il responsabile del trattamento dei dati determina le finalità e i mezzi di trattamento dei dati personali. Dropbox funge da elaboratore di dati per conto della tua organizzazione quando utilizzi Dropbox Business o Dropbox Education; il nostro Contratto Business include gli impegni relativi all'elaborazione dei dati e al trasferimento internazionale di dati.

Il nostro track record: la compliance

La compliance è un ottimo modo per testare l'affidabilità di un servizio. Incoraggiamo e siamo lieti di fornire una verifica indipendente delle nostre pratiche in materia di sicurezza e privacy in merito al rispetto degli standard e delle normative più accettate, come ISO 27001, ISO 27017, ISO 27018, BSI C5 in Germania e SOC 1, 2 e 3. Ad esempio, siamo stati tra i primi provider di servizi cloud ad ottenere la certificazione ISO 27018, lo standard riconosciuto a livello internazionale per le principali pratiche in materia di privacy e protezione dei dati nel cloud. I nostri revisori indipendenti di terze parti testano i nostri controlli, fornendo rapporti e opinioni che vengono condivisi con gli utenti laddove possibile.

Si noti che, sebbene lo scopo delle nostre certificazioni e dei nostri rapporti di controllo si riferisca in genere a Dropbox Business e Dropbox Education, la maggior parte dei nostri controlli è applicabile anche agli utenti Dropbox Basic, Plus e Professional. Maggiori informazioni sugli standard che rispettiamo e su come verifichiamo le nostre pratiche sono disponibili sulla nostra pagina Web sulla conformità.

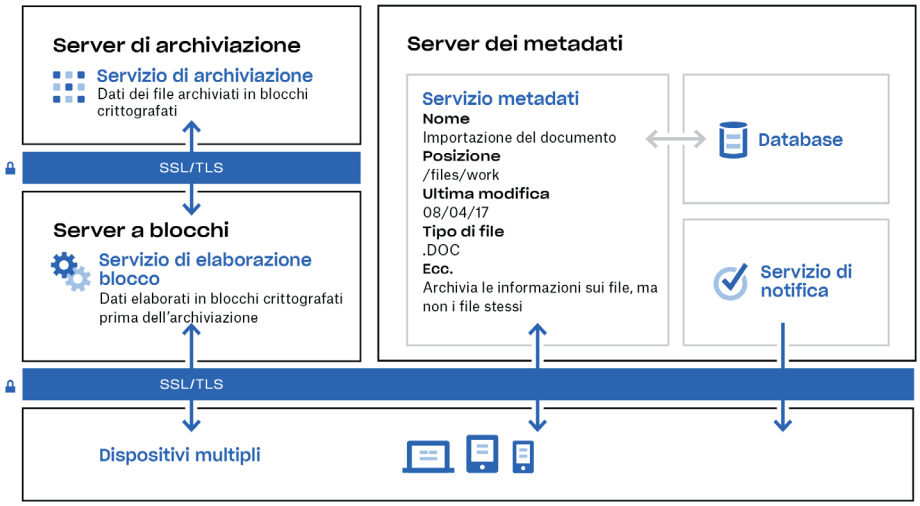
Dropbox

L'architettura Dropbox: proteggere i tuoi dati personali

In Dropbox, crediamo che la protezione dei tuoi dati personali inizi mantenendo i tuoi dati al sicuro. A tal fine, Dropbox è stato progettato con più livelli di protezione, inclusi il trasferimento sicuro dei file di dati, la crittografia e controlli a livello di applicazione, che sono distribuiti attraverso un'infrastruttura sicura e scalabile.

La nostra infrastruttura: i file

L'infrastruttura file di Dropbox è composta dai componenti raffigurati nello schema seguente.



Server a blocchi

A livello di progettazione, Dropbox fornisce un meccanismo di sicurezza davvero unico che va oltre la tradizionale crittografia per proteggere i dati degli utenti. I server a blocchi elaborano i file dalle applicazioni Dropbox dividendoli in blocchi,
criptando ciascun blocco di file utilizzando un codice robusto e sincronizzando soltanto i blocchi che sono stati modificati da una revisione all'altra. Quando un'applicazione Dropbox rileva un nuovo file o una modifica a un file esistente, l'applicazione notifica i server a blocchi. I blocchi di file nuovi o modificati sono quindi elaborati e trasferiti ai server di archiviazione.

Server di notifica

Questo servizio separato si occupa di monitorare le eventuali modifiche apportate agli account Dropbox. Attraverso questo servizio specifico non vengono archiviati o trasferiti né file né metadati. Ogni client stabilisce una connessione long poll con il servizio di notifica e attende. Quando viene apportata una modifica a un file di Dropbox, il servizio di notifica informa i client pertinenti dell'avvenuta modifica chiudendo la connessione long poll. La chiusura della connessione segnala al client che deve collegarsi in modo sicuro al servizio metadati per sincronizzare le modifiche.

Server di metadati

Alcune informazioni di base sui dati dell'utente, chiamate metadati, vengono conservate in un servizio di archiviazione separato che funge da
indice per i dati degli account degli utenti. Tutti i metadati Dropbox vengono archiviati in un servizio di database basato su MySQL, che viene frammentato e replicato secondo le necessità per rispondere ai requisiti relativi a prestazioni ed elevata disponibilità. I metadati includono informazioni di base su account e utenti, come indirizzo e-mail, nome e nomi dei dispositivi. I metadati includono anche
informazioni di base sui file, ad esempio i nomi e i tipi di file, che consentono di supportare funzioni quali la cronologia delle versioni, il ripristino e la sincronizzazione.

Server di archiviazione

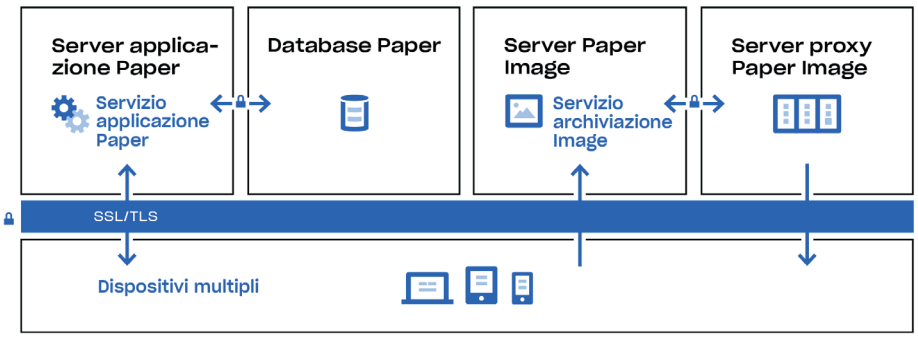
Una volta che i file sono stati suddivisi in blocchi e crittografati dai server a blocchi, il contenuto effettivo di tali blocchi di file viene memorizzato nei server di archiviazione. I server di archiviazione funzionano come un sistema Content-Addressable Storage (CAS), in cui ogni singolo blocco del file crittografato viene recuperato sulla base del suo valore hash.

Per maggiori dettagli sulle funzionalità e sulle norme di sicurezza, consulta il Whitepaper sulla sicurezza di Dropbox Security o contatta sales@dropbox.com

Dropbox

La nostra infrastruttura: Paper

Dropbox Paper (Paper) è una funzione di Dropbox. Tuttavia, Paper utilizza un insieme di sistemi per lo più distinto all'interno dell'infrastruttura di Dropbox. L'infrastruttura file di Dropbox è composta dai componenti raffigurati nello schema seguente.



Server dell'applicazione Paper

I server dell'applicazione Paper elaborano le richieste degli utenti, restituiscono all'utente l'output dei documenti cartacei modificati ed eseguono servizi di notifica. Le sessioni di comunicazione tra i server dell'applicazione Paper e i database di Paper vengono crittografate utilizzando un codice robusto.

Server proxy per le immagini di Paper

Il servizio proxy per le immagini di Paper fornisce un'anteprima sia delle immagini caricate su documenti di Paper, sia dei collegamenti ipertestuali incorporati nei documenti di Paper. Per le immagini caricate in documenti di Paper, il servizio Paper Image Proxy recupera i dati di immagine memorizzati nei server per le immagini di Paper tramite un canale crittografato. Per i collegamenti ipertestuali incorporati nei documenti di Paper, il servizio Paper Image Proxy recupera i dati dell'immagine dal collegamento di origine ed esegue il rendering di un'anteprima dell'immagine tramite HTTP o HTTPS, come specificato dal collegamento di origine.

Database di Paper

Il contenuto effettivo dei documenti Paper degli utenti, così come determinati metadati relativi a tali documenti, sono crittografati nella memoria permanente sui database di Paper. Ciò include informazioni su un documento di Paper (come ad esempio il titolo, l'appartenenza condivisa e le autorizzazioni, le associazioni di cartelle e altre informazioni), nonché i contenuti del documento stesso, inclusi commenti e attività. I database di Paper vengono frammentati e replicati secondo le necessità per rispondere ai requisiti relativi a prestazioni ed elevata disponibilità.

Server di immagini di Paper

Le immagini caricate nei documenti di Paper sono archiviate e crittografate a riposo sui server di immagini di Paper. La trasmissione di dati di immagine tra l'applicazione di paper e i server di immagini di Paper avviene in una sessione crittografata.

Dropbox

Controlli di Dropbox: le nostre prassi interne

Adottiamo misure esaustive per proteggere la nostra infrastruttura, la nostra rete e le nostre applicazioni, formare i dipendenti sulle pratiche in ambito di sicurezza e privacy e costruire una cultura in cui conquistare la fiducia dei clienti è la massima priorità. Di seguito sono descritte in dettaglio alcune delle nostre misure di controllo:

Formazione

Parte della garanzia di protezione dei dati personali dei nostri utenti consiste nel diffondere e favorire la conoscenza delle nozioni di sicurezza e privacy. A questo proposito, ai dipendenti di Dropbox viene richiesta l'accettazione delle norme di sicurezza, incluse le Norme sulla privacy dei dati, prima ancora di ottenere l'autorizzazione ad accedere ai sistemi. Inoltre, i dipendenti partecipano a corsi di formazione obbligatori sulla sicurezza e sulla privacy per i nuovi assunti, oltre alla formazione annuale di follow-up e a una sensibilizzazione continua su tali temi mediante e-mail informative, conferenze, presentazioni e risorse disponibili sulla nostra rete intranet.

Crittografia in transito

Per proteggere i file di dati in transito tra un client Dropbox (al momento desktop, mobile, API o web) e i server front-end di Dropbox,
la connessione è sempre crittografata per garantire la massima sicurezza durante la trasmissione. Allo stesso modo, la connessione è sempre crittografata anche per proteggere i documenti di Paper in transito tra un client Paper (al momento mobile, API o web) e il servizio in hosting. Tali connessioni sono crittografate attraverso la tecnologia Secure Sockets Layer (SSL)/Transport Layer Security (TLS), creando un tunnel sicuro protetto dalla crittografia Advanced Encryption Standard (AES) a 128 bit o superiore.

Crittografia a riposo

I file caricati dagli utenti vengono archiviati nei server di archiviazione di Dropbox in blocchi di file discreti. Ogni blocco viene criptato con Advanced Encryption Standard (AES) a 256 bit. Solo i blocchi modificati tra una revisione e l'altra vengono sincronizzati. Allo stesso modo, anche i documenti di Paper archiviati sui database di Paper vengono crittografati a riposo con lo standard AES a 256 bit.

Eliminazione definitiva di file e documenti di Paper

Quando un utente Dropbox o un amministratore di un team Dropbox Business o Dropbox Education contrassegna un file per l'eliminazione definitiva, si avvia un processo per eliminare definitivamente il file. Allo stesso modo, quando un utente o un amministratore di un team Dropbox Business o Dropbox Education contrassegna un documento di Paper per l'eliminazione definitiva, si avvia un processo simile per eliminare definitivamente dati e immagini del documento di Paper.

Richieste di accesso a dati personali

Per informazioni aggiuntive sui file e i documenti di Paper archiviati con Dropbox, gli utenti possono accedere al sito Web e consultare la pagina del proprio account. La pagina dell'account mostra informazioni come il nome e l'indirizzo e-mail associati all'account. Gli utenti possono anche visualizzare gli indirizzi IP delle sessioni, dei computer e dei dispositivi mobili connessi, nonché le app connesse ai propri account dalla pagina di sicurezza e dalla pagina delle applicazioni connesse.

Gli utenti Dropbox hanno anche la possibilità di richiedere l'accesso o la cancellazione di altri dati personali raccolti su di loro. Ulteriori informazioni su questo processo sono disponibili nel Centro assistenza Dropbox.

Procedure di richiesta di dati da parte di autorità governative. Sappiamo bene che, quando gli utenti ci affidano i propri dati personali, si aspettano che ne manteniamo la riservatezza. Come la maggior parte dei servizi online, Dropbox riceve talvolta richieste da parte di agenzie governative che cercano informazioni sui propri utenti.

I principi seguenti descrivono il modo in cui gestiamo le richieste di dati ricevute da parte di agenzie governative.

Essere trasparenti

Crediamo che ai servizi online debba essere consentito di pubblicare il numero e la tipologia delle richieste governative ricevute e di informare i soggetti interessati della richiesta di informazioni che li riguardano. Questo tipo di trasparenza aiuta agli utenti a comprendere meglio le istanze e i modelli di rischio con gli enti pubblici. Continueremo a pubblicare informazioni dettagliate su queste richieste e a difendere il diritto di fornire informazioni sempre più importanti di questo tipo.

Rifiutare richieste di portata globale

Le richieste di dati da parte di enti governativi devono essere limitate ai dati necessari, essere indirizzate a persone specifiche e giustificate da legittime indagini. Ci opporremo a qualsiasi richiesta di portata eccessivamente ampia.

Fornire servizi affidabili

La pubblica autorità non deve mai installare backdoor nei servizi online o violare l'infrastruttura per ottenere i dati degli utenti. Continueremo a lavorare per proteggere i nostri sistemi e per cambiare le leggi affinché sia chiaro che questo tipo di attività sia da considerarsi illegale.

Proteggere tutti gli utenti

Le norme che garantiscono alle persone tutele diverse in base al luogo in cui vivono o la loro cittadinanza sono obsolete e non riflettono la natura globale dei servizi online. Continueremo a sostenere la riforma di queste leggi.

Questi principi, insieme al nostro rapporto annuale sulla trasparenza, sono resi pubblicamente disponibili sul sito Web Dropbox all'indirizzo: https://www.dropbox.com/transparency.

Per ulteriori dettagli sui nostri controlli e sul nostro approccio alla protezione dei dati personali, consulta il Whitepaper sulla sicurezza di Dropbox Business.

Soggetti terzi che collaborano con Dropbox

Dropbox gestisce in prima persona la maggior parte delle attività relative alla fornitura dei propri servizi; tuttavia, si avvale di alcune terze parti fidate in relazione ai servizi offerti, quali fornitori di assistenza clienti e servizi IT, che accedono alle tue informazioni solo per eseguire attività per nostro conto in conformità con le nostre Norme sulla privacy. Dropbox ne assicura il trattamento in conformità con le proprie istruzioni. Ogni parte terza passa attraverso un rigoroso processo di controllo, incluse verifiche in materia di sicurezza e revisioni contrattuali periodiche, per valutarne la di rispettare i nostri impegni di protezione dei dati.

Trasferimento internazionale di dati

Dropbox fa affidamento su un'ampia gamma di meccanismi legali per il trasferimento internazionale di dati personali dall'UE agli Stati Uniti. Dropbox ha ricevuto la certificazione Privacy Shield Program EU-USA e Svizzera-USA per la raccolta, l'uso e la conservazione di dati personali e il loro trasferimento dall'UE e dalla Svizzera verso gli Stati Uniti. Oltre a ciò, Dropbox offre anche solide garanzie contrattuali sulla privacy dei propri servizi e si affida a clausole contrattuali di tipo UE per il trasferimento internazionale di dati.

Dropbox

GDPR: il Regolamento generale sulla protezione dei dati

Il Regolamento generale sulla protezione dei dati, o GPDR, è un regolamento dell'Unione Europea che stabilisce un nuovo quadro normativo per la protezione dei dati personali dei cittadini dell'UE. Il GDPR rappresenta la parte più significativa della legislazione europea in materia di protezione dei dati dopo la Direttiva sulla protezione dei dati dell'UE del 1995; molte aziende, tra cui Dropbox, che operano in Europa hanno investito molto nella conformità al GDPR.

Il GDPR ha l'obiettivo di armonizzare e portare le leggi sulla protezione dei dati in tutta Europa al passo con i rapidi cambiamenti tecnologici avvenuti negli ultimi due decenni. Il regolamento si basa su precedenti quadri giuridici europei, compresa la Direttiva sulla protezione dei dati dell'UE, introducendo nuovi obblighi e responsabilità per le organizzazioni che trattano dati personali e nuovi diritti per le persone in merito ai propri dati personali. Le organizzazioni con sede nell'UE, così come le organizzazioni che trattano dati personali di residenti nell'UE, sono tenute a rispettare il GDPR.

Dropbox verso la conformità con il GDPR

Dropbox s'impegna a garantire la conformità con il GDPR. Il rispetto della privacy e della sicurezza è un aspetto vitale della nostra attività sin dall'inizio; man mano che siamo cresciuti, la nostra attenzione al trattamento e alla protezione dei dati che i nostri utenti ci affidano è rimasta una priorità. Dropbox è nota per essere all'avanguardia rispetto alla curva di conformità. Come descritto sopra, siamo stati tra i primi fornitori di servizi cloud a ottenere la certificazione ISO 27018 per i nostri utenti aziendali. Data questa solida base, Dropbox considera la conformità con il GDPR un'evoluzione delle pratiche e nei controlli esistenti.

Il percorso di Dropbox verso la conformità con il GDPR è iniziato non appena il regolamento è stato adottato nel 2016. Il nostro primo passo è stato formare un team trasversale di specialisti della protezione dei dati composto da consulenti legali, professionisti della sicurezza e della conformità e product/infrastructure engineer. Il nostro team ha quindi completato una valutazione completa delle nostre attuali pratiche di sicurezza e protezione dei dati rispetto alle disposizioni del GDPR. Il nostro prossimo passo è stato eseguire una valutazione delle nostre attività di trattamento dei dati personali e tracciare il ciclo di vita dei dati personali attraverso i nostri sistemi. A volte queste operazioni vengono definite come "mapping dei dati" e integrano le valutazioni dell'impatto sulla protezione dei dati.

Da allora, abbiamo continuato a sviluppare le procedure interne in essere per garantire il rispetto dei principi di responsabilità ai sensi del GDPR. Questo è importante in quanto il GDPR pone una maggiore attenzione sulla documentazione delle decisioni e delle pratiche che riguardano i dati personali.

Dropbox

Responsabilizzare i nostri utenti nell'adozione del GDPR

Dropbox offre funzioni di controllo e visibilità che possono aiutarti a gestire più facilmente gli obblighi di protezione dei dati, inclusi gli obblighi di conformità GDPR. Ovviamente, la conformità GDPR in tutta la tua organizzazione non inizia né termina con la relazione con i tuoi fornitori, come Dropbox. Sebbene le nostre funzionalità possano aiutarti a gestire i tuoi obblighi, non possono garantire la conformità da soli. La conformità GDPR richiede di pensare in modo più ampio a come i dati si muovono intorno e sono protetti nella tua organizzazione. Ogni organizzazione dovrebbe intraprendere i propri passi per raggiungere la conformità, con i fornitori come partner importanti in quel viaggio.

Minimizzazione dei dati

Un elemento importante del nuovo requisito GDPR Privacy by Design è che le organizzazioni devono progettare i propri servizi in modo da minimizzare i dati. Ciò significa avere una buona visibilità e un buon controllo dei dati all'interno della propria organizzazione per riuscire a gestirli. La dashboard amministratore di Dropbox è uno strumento utile, poiché consente di monitorare l'attività del team, visualizzare i dispositivi connessi e controllare le attività di condivisione.

Protezione e ripristino dei dati

La protezione dei dispositivi smarriti, la cronologia delle versioni e il ripristino dei file possono tutelare da perdite, danni o distruzioni accidentali di dati personali e possono aiutare a ripristinare la disponibilità e l'accesso ai dati personali in modo tempestivo in caso di incidente. L'autenticazione a due fattori è un'altra misura importante che ti consigliamo per proteggere i tuoi dati.

Tenuta di registri

Il GDPR aumenta anche gli obblighi di tenuta di registri dettagliati sulle attività di trattamento svolte dalle organizzazioni. I nostri registri di audit e i nostri registri delle attività possono aiutarti a comprendere meglio le attività di trattamento svolte per favorire la tenuta di registri.

Accesso amministrativo

All'interno della dashboard amministratore di Dropbox, puoi gestire facilmente l'accesso dei membri del team a file, cartelle e documenti di Paper. Per i collegamenti a file condivisi, la nostra funzione di autorizzazione ti consente di proteggere con password i collegamenti condivisi, impostare date di scadenza per concedere un accesso temporaneo e limitare l'accesso ai soli membri dell'organizzazione. Nel caso in cui le responsabilità degli utenti cambino, il nostro strumento per il trasferimento di account consente di trasferire facilmente file e proprietà dei documenti di Paper da un utente a un altro. Gli amministratori hanno anche la possibilità di disattivare l'accesso di un utente al proprio account salvando i relativi dati e le relazioni di condivisione al fine di mantenere al sicuro le informazioni aziendali. Infine, la funzione di pulizia remota consente di eliminare file e documenti di Paper dai dispositivi smarriti o rubati.

Infrastruttura UE

Sebbene nella maggior parte dei casi il GDPR non richieda l'hosting dei dati personali all'interno dell'UE, Dropbox offre a clienti qualificati di Dropbox Business e Dropbox Education la possibilità di archiviare (blocchi di) file nell'UE. L'archiviazione di file nell'UE avviene sull'infrastruttura Amazon Web Services (AWS). Per saperne di più sulla nostra infrastruttura UE, contatta il nostro team di vendita.

Per maggiori dettagli sulle funzionalità e sulle norme di sicurezza, consulta il Whitepaper sulla sicurezza di Dropbox Security o contatta sales@dropbox.com

Dropbox

Collaborare per proteggere i tuoi dati personali

Dropbox lavora con i propri clienti per mantenere al sicuro i loro dati. Adottiamo misure esaustive per proteggere la nostra infrastruttura, la nostra rete e le nostre applicazioni, per formare i dipendenti sulle pratiche in ambito di sicurezza e privacy, per costruire una cultura in cui conquistare la fiducia dei clienti è la massima priorità e per sottoporre i nostri sistemi e le nostre pratiche ad analisi e controlli rigorosi di terze parti.

Tuttavia, anche gli utenti svolgono un ruolo chiave nell'assicurarsi che i loro dati personali siano protetti. Dropbox ti consente di configurare, utilizzare e monitorare il tuo account in modo da soddisfare le esigenze di sicurezza, privacy e conformità della tua organizzazione. La nostra guida alla responsabilità condivisa può aiutarti a capire meglio ciò che facciamo per tenere al sicuro il tuo account e ciò che puoi fare per conservare la visibilità e il controllo sui dati del tuo team.

Riepilogo

Ogni giorno, milioni di utenti si affidano a Dropbox. Per essere degni di tale fiducia, abbiamo creato e continueremo a far crescere Dropbox dedicando particolare attenzione alla sicurezza e alla privacy. Il nostro impegno a proteggere i dati personali dei nostri utenti è al centro di ogni decisione che prendiamo. Per saperne di più, invia un'e-mail all'indirizzo privacy@dropbox.com. Per maggiori informazioni sul GDPR, puoi anche visitare il nostro centro di orientamento al GDPR.