Dropbox

Privacy e protezione dei dati

Introduzione

I dati personali hanno un ruolo molto importante nella società e nell'economia. Sempre più persone cercano maggiore controllo e chiarezza su come i propri dati vengono utilizzati e tutelati dalle organizzazioni con cui interagiscono.

In Dropbox, la fiducia è alla base del nostro rapporto con milioni di persone e aziende di 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. I Termini di Servizio di Dropbox definiscono le tue responsabilità quando utilizzi i nostri servizi. La nostra Normativa sulla Privacy descrive il nostro impegno verso la privacy degli utenti e spiega come raccogliamo, utilizziamo e gestiamo i tuoi dati personali quando utilizzi i nostri servizi. Se sei residente in Nord America (Stati Uniti, Canada e Messico), Dropbox, Inc. costituisce il tuo fornitore di servizi.

Per tutti gli altri utenti, Dropbox International Unlimited Company agisce come responsabile dei tuoi dati personali.

Se sei un utente Dropbox Business o Dropbox Education, la tua organizzazione agisce come responsabile di tutti i dati forniti a Dropbox attraverso il tuo utilizzo di Dropbox Business o Dropbox Education. Il responsabile dei dati determina le finalità e le modalità di trattamento dei dati personali. Dropbox agisce come responsabile dei dati personali, trattando i dati per conto della tua organizzazione quando utilizzi Dropbox Business o Dropbox Education; il nostro Contratto di Business include gli impegni relativi al trattamento dei dati e al trasferimento internazionale dei dati.

Il nostro registro di tracciabilità: compliance

La compliance rappresenta un modo efficace per verificare l'affidabilità di un servizio. Incoraggiamo e siamo lieti di fornire una verifica indipendente che le nostre pratiche di sicurezza e privacy siano conformi agli standard e alle normative più diffusi, come ISO 27001, ISO 27017, ISO 27018, HIPPA/HITECH, Germania BSI C5 e SOC 1, 2 e 3.

Inoltre, siamo stati tra i primi fornitori di servizi cloud a ottenere la certificazione ISO 27018, lo standard riconosciuto a livello internazionale per le principali pratiche in materia di privacy e protezione dei dati. I nostri revisori esterni indipendenti testano i nostri controlli e forniscono report e opinioni che condividiamo con gli utenti quando possibile.

Mentre l'ambito delle nostre certificazioni e dei rapporti di audit fa generalmente riferimento a Dropbox Business e Dropbox Education, la maggior parte dei nostri controlli è applicabile anche agli utenti di Dropbox Basic, Plus e Professional. Ulteriori informazioni sugli standard a cui aderiamo e con cui verifichiamo le nostre pratiche sono disponibili sulla nostra pagina web dedicata alla compliance.

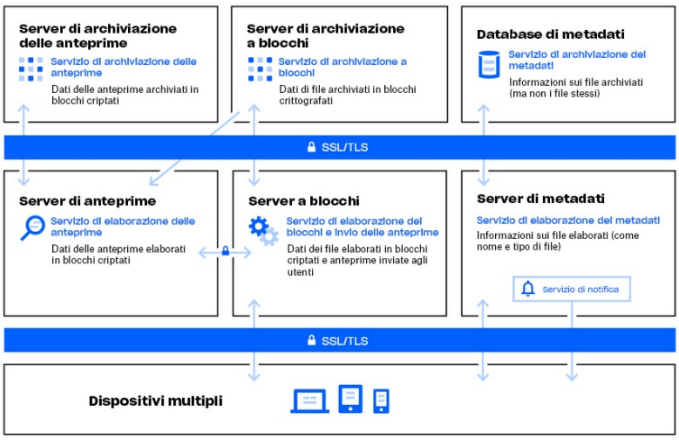
Dropbox

Architettura di Dropbox: protezione dei tuoi dati personali

In Dropbox, crediamo che la protezione dei tuoi dati personali inizi dal mantenerli al sicuro. A questo proposito, Dropbox è stato progettato con più livelli di protezione, che includono il trasferimento sicuro dei dati, la crittografia, la configurazione di rete e controlli a livello di applicazione, distribuiti attraverso un'infrastruttura sicura e scalabile.

La nostra infrastruttura: i file

L'infrastruttura per i file di Dropbox comprende i componenti descritti nel diagramma di seguito.



Server di metadati

Alcune informazioni di base sui dati dell'utente, chiamate metadati, vengono conservate nel rispettivo servizio di archiviazione discreto e fungono da indice per i dati negli account degli utenti. Tra i metadati rientrano le informazioni di base sull'account e sull'utente, come l'indirizzo e-mail, il nome e il tipo di dispositivo utilizzato. I metadati includono anche le informazioni di base sui file, compresi nomi e tipi di file, che aiutano a supportare le funzioni come la cronologia delle versioni, il recupero e la sincronizzazione.

Database di metadati

I metadati dei file sono archiviati in un servizio di database My-SQL e vengono condivisi e replicati secondo le necessità per rispondere ai requisiti relativi a prestazioni ed elevata disponibilità.

Server a blocchi

Per impostazione predefinita, Dropbox fornisce un meccanismo di sicurezza unico che va oltre la tradizionale crittografia per proteggere i dati dell'utente. I server a blocchi elaborano i file delle applicazioni Dropbox dividendo ogni file in blocchi, criptando ogni blocco utilizzando una cifratura complessa e sincronizzando solo i blocchi che sono stati modificati tra le revisioni. Quando un'applicazione Dropbox individua un nuovo file o una modifica apportata a un file esistente, l'applicazione notifica la modifica al server a blocchi e i blocchi del file nuovi o modificati vengono elaborati e trasferiti al server di archiviazione.

Server di archiviazione a blocchi

I contenuti effettivi dei file degli utenti vengono archiviati in blocchi crittografati all'interno del server. Prima della trasmissione, il client di Dropbox suddivide i file in blocchi per prepararli per l'archiviazione. Il server di archiviazione a blocchi funziona come un sistema Content-Addressable Storage (CAS) e ogni singolo blocco del file crittografato viene recuperato sulla base del suo valore hash.

Server di anteprime

I server di anteprime servono per produrre le anteprime dei file. Le anteprime sono una renderizzazione del file dell'utente in un formato diverso, più adatto alla visualizzazione rapida sul dispositivo dell'utente. I server di anteprime recuperano i blocchi di file dai server di archiviazione a blocchi per generare le anteprime. Quando viene richiesta l'anteprima di un file, i server di anteprime recuperano l'anteprima memorizzata nella cache dai server di archiviazione delle anteprime e la trasferiscono nel server a blocchi. Le anteprime vengono infine trasmesse agli utenti tramite server a blocchi.

Server di archiviazione delle anteprime

Le anteprime memorizzate nella cache sono archiviate in un formato crittografato nei server di archiviazione delle anteprime.

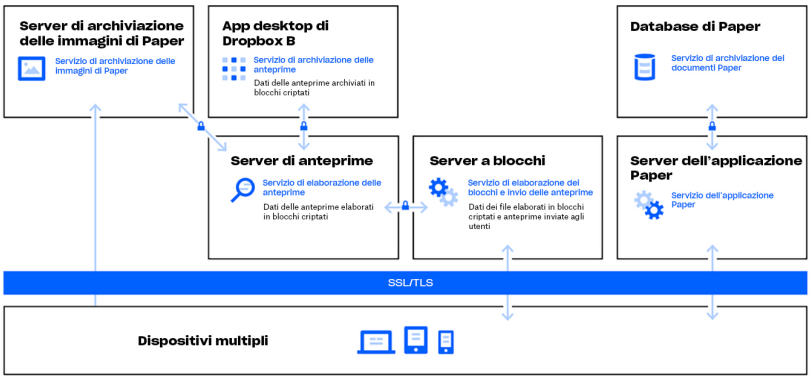
Servizio di notifica

Questo è un servizio distinto dedicato a controllare se sono state effettuate modifiche agli account Dropbox. File e metadati non vengono archiviati o trasferiti attraverso questo servizio specifico. Ogni client stabilisce una connessione long poll con il servizio di notifica e attende. Quando si verifica una modifica in qualsiasi 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 server di metadati per sincronizzare le modifiche.

Dropbox

La nostra infrastruttura: Paper

Dropbox Paper (Paper) è una funzione del prodotto Dropbox. Tuttavia, Paper utilizza per lo più un set distinto di sistemi all'interno dell'ambiente dell'infrastruttura Dropbox. L'infrastruttura di Paper fa parte dei componenti descritti nel diagramma di seguito.



Application server di Paper

Gli application server di Paper elaborano le richieste degli utenti, eseguono il rendering dell'output dei documenti di Paper modificati per l'utente ed eseguono servizi di notifica. Gli application server di Paper scrivono le modifiche in entrata degli utenti nei database di Paper, dove sono disposti in uno spazio di archiviazione persistente. Le sessioni di comunicazione tra gli application server e i database di Paper vengono crittografate con un codice robusto.

Database di Paper

I contenuti effettivi dei documenti di Paper degli utenti, così come determinati metadati su tali documenti, vengono crittografati in uno spazio di archiviazione continuo nei database di Paper. Tali contenuti comprendono informazioni su un documento di Paper (ad esempio titolo, iscrizioni e autorizzazioni condivise, associazioni di progetti e cartelle e altre informazioni), nonché contenuti all'interno del documento di Paper stesso, compresi commenti e attività. I database di Paper vengono condivisi e replicati secondo le necessità per rispondere ai requisiti relativi a prestazioni ed elevata disponibilità.

Server di archiviazione delle immagini di Paper

Le immagini caricate nei documenti di Paper vengono archiviate e crittografate durante l'inattività nei server di immagini di Paper. La trasmissione dei dati delle immagini tra l'application server e i server di immagini di Paper avviene nel corso di una sessione crittografata.

Server di anteprime

I server di anteprime creano le anteprime delle immagini caricate nei documenti Paper e dei collegamenti ipertestuali incorporati nei documenti Paper. Per le immagini caricate nei documenti Paper, i server di anteprime recuperano i dati delle immagini archiviati nei server di archiviazione delle immagini di Paper tramite un canale crittografato. Per i collegamenti ipertestuali incorporati nei documenti Paper, i server di anteprime recuperano i dati delle immagini e renderizzano l'anteprima dell'immagine utilizzando la crittografia come specificato dal link originale. Le anteprime vengono infine trasmesse agli utenti tramite i server a blocchi.

Server di archiviazione delle anteprime

Gli utenti Paper utilizzano gli sessi server di archiviazione delle anteprime descritti nel diagramma dell'infrastruttura di Dropbox per archiviare le anteprime delle immagini memorizzate nella cache. I blocchi di anteprime memorizzati nella cache sono archiviati in un formato crittografato nei server di archiviazione delle anteprime.

Dropbox

Controlli di Dropbox: le nostre pratiche interne

Adottiamo misure globali per proteggere la nostra infrastruttura, la nostra rete e le nostre applicazioni. Alcune delle misure di sicurezza che utilizziamo prevedono la crittografia"a riposo", la crittografia in transito e l'eliminazione permanente dei file. Inoltre offriamo una solida formazione in materia di privacy e sicurezza, in modo che i nostri dipendenti possano creare una cultura in cui essere degni di fiducia ha la massima priorità. Di seguito sono descritti i dettagli su alcuni dei nostri controlli.

Formazione

Parte della protezione dei dati personali dei nostri utenti consiste nel creare e coltivare una cultura basata sulla sicurezza e sulla consapevolezza riguardo alla privacy. I dipendenti Dropbox devono accettare le nostre politiche di sicurezza, comprese le norme sulla privacy dei dati degli utenti, prima di ottenere l'accesso al sistema. Solo i dipendenti con esigenze specifiche hanno accesso a tali sistemi.
I dipendenti partecipano inoltre a sessioni di formazione annuali obbligatorie in materia di privacy e sicurezza.

Crittografia in transito

Per proteggere i dati dei file in transito tra un client Dropbox (attualmente desktop, mobile, API o web) e i server front-end si Dropbox, viene negoziata una connessione crittografata per garantire un trasferimento sicuro. Allo stesso modo, viene negoziata una connessione crittografata per proteggere i dati dei documenti Paper in transito tra un client Paper (attualmente desktop, mobile, API o web) e il servizio in hosting. Queste connessioni vengono crittografate utilizzando il protocollo Secure Sockets Layer (SSL)/Transport Layer Security (TLS) per creare un tunnel sicuro protetto da un algoritmo di cifratura Advanced Encryption Standard (AES) a 128 bit o superiore.

Crittografia durante l'archiviazione

I file caricati dagli utenti vengono archiviati sui server di archiviazione di Dropbox come blocchi di file discreti. I file di Dropbox archiviati sono criptati 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 dati dei documenti Paper archiviati nei database di Paper vengono crittografati a riposo utilizzando l'algoritmo di cifratura Advanced Encryption Standard (AES) a 256 bit.

Eliminazione permanente di file e documenti Paper

Quando un utente Dropbox o l'amministratore di un team Dropbox Business o Dropbox Education seleziona un file per eliminarlo definitivamente, avvia un processo di cancellazione permanente di un file. Allo stesso modo, quando un utente Dropbox o l'amministratore di un team Dropbox Business o Dropbox Education seleziona un file Paper per eliminarlo definitivamente, viene avviato un processo simile per eliminare in modo permanente i dati del documento di Paper e delle immagini.

Richieste di accesso ai dati personali

Per ottenere l'accesso ai dati personali, nonché ai file e ai documenti Paper archiviati su Dropbox, gli utenti possono aprire il sito web e accedere alla pagina del proprio account. Nella pagina dell'account sono presenti informazioni come il nome e l'indirizzo e-mail associati all'account. Gli utenti possono inoltre visualizzare gli indirizzi IP delle sessioni connesse, oltre ai computer, ai dispositivi mobili e alle app connessi al proprio account dalla pagina di sicurezza e dalla pagina delle applicazioni connesse.

Gli utenti di Dropbox hanno anche la possibilità di richiedere l'accesso o l'eliminazione di altri dati personali che Dropbox potrebbe aver raccolto su di loro. Ulteriori informazioni su questo processo sono disponibili nel Centro Assistenza di Dropbox.

Governance della privacy di Dropbox

Il team addetto al Programma sulla privacy di Dropbox è responsabile del funzionamento di tale programma. Si occupa infatti di implementare le nostre iniziative chiave sulla privacy e supporta la privacy "by design" nel nostro ciclo di vita dei dati. Il Programma sulla privacy di Dropbox è ulteriormente supportato da numerosi sotto-team legali polifunzionali. Questi sotto-team forniscono le ulteriori competenze richieste per svolgere e supervisionare le attività quotidiane del Programma sulla privacy.

Il team responsabile della protezione dei dati opera separatamente dalle altre funzioni di privacy e funge da garante di conformità e supervisore della privacy, supportando direttamente il Responsabile della protezione dei dati nell'esercizio delle sue funzioni. Il Responsabile della protezione dei dati è il rappresentante locale dell'UE ed è possibile contattarlo all'indirizzo privacy@dropbox.com.

Dropbox

Principi relativi alle richieste ufficiali di dati

Comprendiamo che quando gli utenti ci affidano i propri dati personali si aspettano che tali dati vengano mantenuti riservati. Come la maggior parte dei servizi online, a volte Dropbox riceve richieste da parte della pubblica autorità volte a ottenere informazioni sui nostri utenti.

I principi elencati di seguito descrivono come gestiamo le richieste da parte della pubblica autorità volte a ottenere dati che riceviamo.

Trasparenza

Riteniamo che ai servizi online dovrebbe essere consentito di pubblicare il numero e le tipologie di richieste ufficiali ricevute e di notificare i singoli utenti quando vengono richieste informazioni relative a essi. Questo tipo di trasparenza responsabilizza le persone, aiutandole a comprendere meglio le istanze e i casi di richieste eccessive da parte della pubblica autorità. Continueremo a pubblicare informazioni dettagliate su queste richieste e a rivendicare il diritto di fornire ulteriori informazioni di tale importanza.

Rifiutare richieste eccessive

Le richieste ufficiali di dati devono limitarsi ai dati che le autorità cercano di ottenere ed essere strettamente mirate a persone specifiche e a indagini giustificate. Ci opporremo a richieste a tappeto o con scopi eccessivi.

Fornitura di 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.

Protezione di tutti gli utenti

Le leggi conferiscono alle persone diversi tipi di protezione in base alla cittadinanza o al luogo di residenza e non riflettono la natura globale dei servizi online. Continueremo a sostenere le riforme di tali leggi.

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

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

Altre figure che lavorano per e con Dropbox

Dropbox gestisce la maggior parte delle attività legate alla fornitura dei nostri servizi; tuttavia, ci affidiamo a terze parti attendibili relativamente ai nostri servizi (ad esempio, tecnici dell'assistenza clienti e servizi IT). Queste terze parti avranno accesso alle tue informazioni solo per eseguire attività per conto nostro in conformità con le nostre Norme sulla Privacy e saranno responsabili della gestione delle tue informazioni in accordo con le nostre istruzioni.

Ciascuna terza parte conduce un rigoroso processo di esame, che comprende valutazioni della sicurezza e revisioni periodiche dei contratti, per valutarne la capacità di rispettare il nostro impegno verso la protezione dei dati.

Trasferimenti internazionali di dati

Per il trasferimento internazionale di dati personali dall'UE agli Stati Uniti, Dropbox si affida a una serie di meccanismi legali. Disponiamo della certificazione dei programmi Privacy Shield UE-USA e Svizzera-USA riguardanti la raccolta, l'utilizzo e la conservazione dei dati personali e il relativo trasferimento dall'UE e dalla Svizzera agli Stati Uniti. Oltre a Privacy Shield, Dropbox offre anche solide garanzie contrattuali sulla privacy dei suoi servizi e ha implementato le clausole contrattuali standard dell'Unione Europea per tutelare i trasferimenti di dati internazionali.

Dropbox

GDPR: Regolamento generale sulla protezione dei dati

Il Regolamento generale sulla protezione dei dati, o GDPR, è un regolamento europeo che stabilisce un nuovo accordo quadro relativo alla protezione dei dati personali per i soggetti interessati residenti nell'UE.

Il GDPR è la parte più significativa della legislazione europea sulla protezione dei dati dalla Direttiva europea sulla protezione dei dati del 1995; come molte altre aziende che operano in Europa, Dropbox ha investito molto nella conformità al GDPR.

Il GDPR armonizza le leggi sulla protezione dei dati in tutta Europa e le mette al passo con i rapidi cambiamenti tecnologici che si sono verificati negli ultimi due decenni.

Questo regolamento si basa su quadri giuridici europei del passato, compresa la Direttiva europea sulla protezione dei dati, e introduce nuovi obblighi e responsabilità per le organizzazioni che gestiscono i dati personali e nuovi diritti per i soggetti interessati rispetto ai loro dati personali. Le organizzazioni con sede nell'UE e le organizzazioni che trattano i dati personali dei soggetti interessati residenti in UE sono tenute a rispettare il GDPR.

Il viaggio di Dropbox verso la compliance al GDPR

Dropbox si impegna a rispettare il GDPR. Il rispetto della privacy e della sicurezza è stato integrato nella nostra attività sin dall'inizio e, man mano che siamo cresciuti, la nostra attenzione per la gestione e la protezione dei dati che ci vengono affidati dai nostri utenti è rimasta una priorità. Dropbox è sempre stata un passo avanti per quanto riguarda la curva di conformità; come scritto sopra, siamo stati tra i primi fornitori di servizi cloud a ottenere la certificazione ISO 27018 per i nostri utenti business. Data questa solida base, Dropbox considera la conformità al GDPR un'evoluzione delle nostre pratiche e dei nostri controlli già esistenti e rappresenta una serie costante e in continua evoluzione di iniziative volte a garantire che i dati personali dei nostri utenti siano sempre protetti.

Il percorso di Dropbox verso la compliance con il GDPR è iniziato nel 2016, con l'adozione del regolamento. Il nostro primo passo è stato formare un team polifunzionale di specialisti della protezione dei dati composto da consulenti legali, professionisti della conformità e della sicurezza e ingegneri delle infrastrutture. Il nostro team ha dunque svolto una valutazione completa delle nostre pratiche di sicurezza e di protezione dei dati in vigore rispetto ai requisiti del GDPR.

Il passo successivo è stato quello di condurre una valutazione delle nostre attività di trattamento dei dati personali e di tracciare il ciclo di vita dei dati personali attraverso i nostri sistemi. Questi esercizi sono talvolta definiti esecuzione della Mappatura dei dati e completamento della Valutazione dell'impatto della protezione dei dati. L'esecuzione è approvata nel contesto della Mappatura dei dati.

Mapping dei dati e completamento delle valutazioni dell'impatto della protezione dei dati.

Da allora, abbiamo continuato a migliorarci basandoci su processi e procedure interni per garantire il rispetto dei principi di responsabilità ai sensi del GDPR. Ciò è importante, poiché il GDPR pone particolare attenzione alla documentazione delle decisioni e delle pratiche che interessano i dati personali.

Dropbox

Preparare i nostri utenti al loro percorso verso il GDPR

Dropbox offre funzioni di controllo e visibilità che possono aiutarti a gestire più facilmente i tuoi obblighi di protezione dei dati, inclusi gli obblighi di conformità al GDPR. Naturalmente, la conformità al GDPR di tutta l'organizzazione non inizia o termina con il rapporto con i tuoi fornitori, come ad esempio Dropbox. Sebbene le nostre funzioni possano aiutarti a gestire i tuoi obblighi, non possono garantire la conformità in sé e per sé. La conformità al GDPR richiede una riflessione più ampia sul modo in cui i dati si spostano e sono protetti all'interno della tua organizzazione. Ogni organizzazione deve intraprendere le misure adeguate per garantire la conformità, guardando ai fornitori come a dei partner importanti in questo percorso.

Minimizzazione dei dati

Un elemento importante del requisito del GDPR "Privacy by Design" consiste nel fatto che le organizzazioni devono progettare i propri servizi in modo tale da minimizzare i dati. Ciò consente di avere buona visibilità e controllo dei dati all'interno dell'organizzazione e pertanto di gestirli più facilmente. La dashboard di amministrazione di Dropbox Business è uno strumento utile in questo senso, in quanto consente di monitorare l'attività del team, visualizzare i dispositivi connessi e valutare l'attività di condivisione. Lavoriamo per implementare i principi di Privacy by Design in nuovi prodotti e funzionalità.

Protezione e ripristino dei dati

La protezione in caso di smarrimento del dispositivo, la cronologia delle versioni e il ripristino dei file possono proteggere gli utenti dalle perdite e dai danni accidentali o dalla distruzione di dati personali e possono essere d'aiuto per ripristinare tempestivamente la disponibilità dei dati personali e l'accesso ad essi in caso di imprevisti. L'autenticazione a due fattori è un'altra importante misura che consigliamo di adottare per proteggere i dati.

Mantenimento dei registri

Il GDPR aumenta l'obbligo per le organizzazioni di mantenere registri dettagliati delle proprie attività di trattamento dei dati. I nostri registri di audit e registri attività possono aiutarti a comprendere meglio le tue attività di trattamento per supportare il mantenimento dei tuoi registri.

Amministrazione degli accessi

Nella dashboard amministratore di Dropbox Business puoi facilmente gestire l'accesso a file, cartelle e documenti Paper da parte dei membri del team. Per quanto riguarda i link ai file condivisi, le nostre funzioni di autorizzazione per i link ti consentono di proteggere i link condivisi tramite password, stabilire date di scadenza per consentire un accesso temporaneo e limitare l'accesso ai membri della tua organizzazione. In caso di modifiche delle responsabilità degli utenti, il nostro strumento di trasferimento degli account ti consente di trasferire i file e la proprietà dei documenti Paper da un utente all'altro.

Gli amministratori hanno inoltre la possibilità di disattivare l'accesso di un utente al suo account, pur mantenendo i dati e i rapporti di condivisione per tenere al sicuro le informazioni sulla tua organizzazione.

Infine, la funzione di cancellazione da remoto ti consente di eliminare i file e i documenti Paper da un dispositivo smarrito o rubato.

Infrastruttura UE

Anche se il GDPR non richiede che i dati personali siano ospitati all'interno dell'UE, Dropbox offre ai clienti Dropbox Business e Dropbox Education idonei la possibilità di archiviare i file (blocchi) in UE. L'archiviazione di file con sede nell'UE viene fornita attraverso l'infrastruttura Amazon Web Services (AWS). Per saperne di più sulla nostra infrastruttura UE, contatta il nostro team di vendita.

Dropbox

Collaborare per proteggere i tuoi dati personali

Dropbox collabora con i suoi utenti per proteggere i loro dati personali. Adottiamo misure globali per proteggere la nostra infrastruttura, la nostra rete e le nostre applicazioni, offriamo ai dipendenti una formazione su pratiche di sicurezza e privacy, creiamo una cultura in cui essere degni di fiducia è la massima priorità e sottoponiamo i nostri sistemi e le nostre pratiche a rigorosi test e valutazioni condotti da terze parti.

Tuttavia, anche gli utenti giocano un ruolo fondamentale nella protezione dei propri dati personali. Dropbox ti consente di configurare, utilizzare e monitorare il tuo account in modi che soddisfano la privacy della tua organizzazione. La nostra Guida sulla responsabilità condivisa può aiutarti a capire di più su ciò che facciamo per mantenere il tuo account al sicuro e su ciò che puoi fare per avere visibilità e controllo sui tuoi dati personali.

Riepilogo

Ogni giorno, milioni di utenti si affidano a Dropbox. Per essere degni di tale fiducia, abbiamo creato e continuiamo a far crescere Dropbox ponendo particolare attenzione su sicurezza e privacy. Il nostro impegno verso la protezione dei dati personali dei nostri utenti è al centro di ogni decisione che prendiamo. Per ulteriori informazioni, scrivi un'e-mail all'indirizzo privacy@dropbox.com. Per ulteriori informazioni sul GDPR, puoi anche visitare il nostro centro GDPR.