Dropbox

Privacy e protezione dei dati

Introduzione

I dati personali giocano un ruolo fondamentale 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 tutelati dalle organizzazioni con cui interagiscono.

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 il nostro impegno verso la privacy degli utenti e spiegano come raccogliamo, utilizziamo e gestiamo i tuoi dati personali quando utilizzi i nostri servizi. Se risiedi in Nord America (Stati Uniti, Canada e Messico), Dropbox, Inc. agisce come fornitore di servizi. Per tutti gli altri utenti, Dropbox International Unlimited Company agisce come titolare del trattamento dei dati personali.

Se sei un utente Dropbox Business o Dropbox Education, la tua organizzazione agisce come titolare 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 agisce come responsabile del trattamento dei dati, elaborando i dati per conto della tua organizzazione quando utilizzi Dropbox Business o Dropbox Education, mentre il nostro Contratto di Business comprende gli impegni relativi al trattamento dei dati e al trasferimento internazionale dei dati.

Il nostro track record: la conformità

La conformità 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 diffuse, come ISO 27001, ISO 27017, ISO 27018, ISO 27701, HIPPA/HITECH e SOC 1, 2 e 3.

Ad esempio, siamo stati tra i primi provider 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 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. È importante tenere conto che, sebbene le nostre certificazioni e i nostri rapporti di audit facciano 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. Inoltre, ora Dropbox aderisce al Codice di condotta dell'Unione Europea sul cloud. Ulteriori informazioni sugli standard a cui aderiamo e con cui verifichiamo le nostre pratiche sono disponibili sulla nostra pagina web dedicata alla conformità.

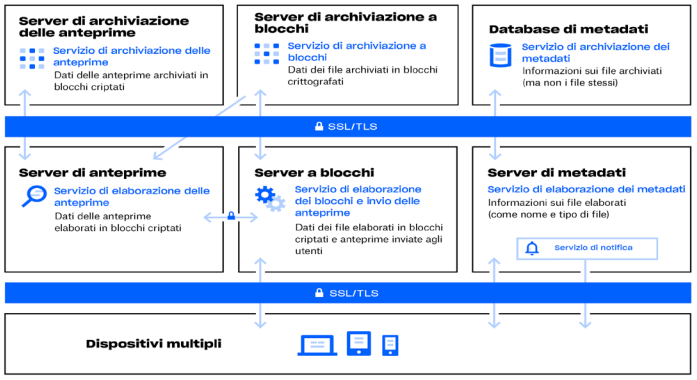
Dropbox

L'architettura Dropbox: proteggere i tuoi dati personali

In Dropbox, crediamo che la protezione dei tuoi dati personali inizi mantenendoli 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 i controlli a livello di applicazione, che sono distribuiti attraverso un'infrastruttura sicura e scalabile.

La nostra infrastruttura: file

L'infrastruttura dei file di Dropbox comprende i componenti raffigurati nello schema seguente.



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. I metadati includono informazioni di base su account e utenti, come indirizzo email, 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 funzionalità quali la cronologia delle versioni, il ripristino e la sincronizzazione.

Database di metadati

Tutti i metadati dei file vengono archiviati in un servizio di database basato su MySQL, che viene frammentato e replicato secondo necessità per soddisfare i requisiti relativi a prestazioni ed elevata disponibilità.

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 archiviazione a blocchi

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

Server di anteprime

I server di anteprima servono per produrre le anteprime dei file. Le anteprime consistono in un rendering dei file di un utente in un formato file diverso, più adatto a una visualizzazione rapida sul dispositivo dell'utente finale. 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 di anteprime e la trasferiscono al server a blocchi. Le anteprime vengono infine mostrate agli utenti tramite i server a blocchi.

Server di archiviazione delle anteprime

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

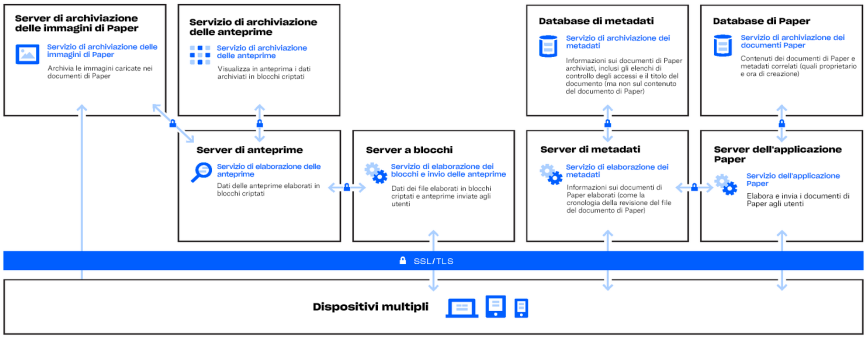
Servizio di notifica

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.

Dropbox

La nostra infrastruttura: Paper

Dropbox Paper (Paper) è una funzionalità 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. I server dell'applicazione Paper scrivono le modifiche degli utenti in entrata nei database di Paper, dove vengono inserite in uno spazio di archiviazione permanente. Le sessioni di comunicazione tra i server dell'applicazione Paper e i database di Paper vengono crittografate utilizzando un codice robusto.

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, compresi commenti e attività. I database di Paper vengono frammentati e replicati secondo necessità per rispondere ai requisiti relativi a prestazioni ed elevata disponibilità.

Server di archiviazioni 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.

Server di anteprime

I server di anteprime forniscono 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, i server di anteprime recuperano 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, i server di anteprime recuperano i dati dell'immagine dal collegamento di origine ed eseguono il rendering di un'anteprima dell'immagine tramite HTTP o HTTPS, come specificato dal collegamento di origine. Le anteprime vengono infine mostrate agli utenti tramite i server a blocchi.

Server di archiviazione di anteprime

Paper utilizza gli stessi server di archiviazione di anteprime descritti nel diagramma dell'infrastruttura di Dropbox per archiviare le anteprime delle immagini salvate nella cache. Le anteprime memorizzate nella cache vengono archiviate in un formato crittografato nei server di archiviazione delle anteprime.

Dropbox

Controlli Dropbox: le nostre pratiche interne

Adottiamo misure esaustive per proteggere la nostra infrastruttura, la nostra rete e le nostre applicazioni. Tra le misure di sicurezza che applichiamo rientrano la crittografia dei dati a riposo e in transito e l'eliminazione permanente dei file. Inoltre offriamo ai dipendenti una valida formazione sulle pratiche in ambito di sicurezza e privacy per creare una cultura in cui conquistare la fiducia dei clienti è la massima priorità. Di seguito sono descritte nel 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. Solo i dipendenti con una necessità specifica hanno accesso a tali sistemi. I dipendenti partecipano inoltre a corsi di formazione obbligatori in materia di sicurezza e privacy a cadenza annuale.

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, in modo da 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 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 a dati personali

Per ottenere l'accesso ai dati personali, nonché ai file e ai documenti di Paper archiviati in Dropbox, gli utenti possono accedere al sito web e andare alla pagina del proprio account. La pagina dell'account mostra informazioni come il nome e l'indirizzo email associati all'account. Gli utenti possono anche visualizzare gli indirizzi IP delle sessioni, dei computer e dei dispositivi mobili connessi, nonché le app connesse al proprio account dalla pagina sulla 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.

Governance della privacy in Dropbox

Il tteam che si occupa della privacy è responsabile del funzionamento del Programma per la privacy di Dropbox; implementa le nostre principali iniziative in materia di privacy e supporta il principio di Privacy by Design nel nostro ciclo di vita dei dati. Il Programma per la privacy di Dropbox è ulteriormente supportato da diversi team secondari legali polifunzionali. Questi sottogruppi offrono ulteriori competenze necessarie per eseguire e supervisionare le attività quotidiane del Programma per la privacy.

Il team DPO opera separatamente dalle altre funzioni inerenti alla privacy e ha il compito di garantire conformità in materia di privacy, oltre che di supervisionare, collaborando direttamente con il responsabile della protezione dei dati nell'esecuzione delle proprie mansioni. È possibile contattare il responsabile della protezione dei dati (DPO) all'indirizzo privacy@dropbox.com.

Dropbox

Dati governativi

Principi relativi alle richieste

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 gli utenti a comprendere meglio le istanze e i limiti entro i quali possono spingersi gli enti governativi. Continueremo a pubblicare informazioni dettagliate su queste richieste e a difendere il diritto di fornire sempre più importanti informazioni di questo tipo.

Respingere le richieste eccessive

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.

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 è da considerarsi illegale.

Proteggere tutti gli utenti

Le norme che garantiscono alle persone tutele diverse in base al luogo in cui vivono o alla 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.

Ciascuna terza parte segue un rigoroso processo di controllo, che comprende revisioni delle norme di sicurezza e privacy e revisioni periodiche del contratto, per valutare la propria capacità di adempiere ai nostri obblighi di protezione dei dati. Sulla base di questi processi di controllo, Dropbox afferma che le sue terze parti di fiducia si impegnano a rispettare le leggi dell'Unione Europea sulla protezione dei dati applicabili in relazione al trattamento dei dati personali per conto di Dropbox. I clienti possono monitorare le terze parti fidate di Dropbox esaminando le certificazioni ISO 27001 e 27018 di Dropbox e, in base agli opportuni obblighi di riservatezza, esaminando il report SOC 2 Type II di Dropbox. In particolare, i clienti possono monitorare i partner terzi attendibili di Dropbox esaminando i risultati dei controlli e degli audit di Dropbox in base ai criteri Trust Services P6.1, P6.4 e CC.9.2 del report SOC 2 Type II.

Dropbox

Trasferimento internazionale di dati

Nel trasferire dati dall'Unione Europea, dallo Spazio economico europeo, dal Regno Unito e dalla Svizzera, Dropbox si affida a una serie di meccanismi legali, inclusi i contratti con i propri clienti e affiliati, le Clausole contrattuali standard e le decisioni di adeguatezza della Commissione europea in merito a determinati Paesi, a seconda dei casi.

Dropbox è conforme ai Quadri sulla privacy dei dati UE-USA e Svizzera-USA, nonché all'Estensione del Regno Unito al Quadro sulla privacy dei dati UE-USA, come stabilito dal Dipartimento del Commercio degli Stati Uniti per quanto riguarda il trattamento dei dati personali provenienti dall'Unione Europea, dallo Spazio Economico Europeo, dal Regno Unito e dalla Svizzera e trasferiti agli Stati Uniti. Dropbox ha certificato al Dipartimento del Commercio degli Stati Uniti la propria adesione ai principi di questi Quadri sulla privacy dei dati per quanto riguarda tali dati, senza però includere in tale certificazione la parte dei Servizi relativa a DocSend o Formswift.

Per ulteriori informazioni sul Quadro sulla privacy dei dati e per visualizzare la certificazione di Dropbox, visita www.dataprivacyframework.gov.

Eventuali reclami e controversie relativi alla nostra conformità al Quadro sulla privacy dei dati vengono esaminati e risolti tramite JAMS, una terza parte indipendente. Per ulteriori informazioni, consulta le nostre Norme sulla privacy.

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 quadro normativo per la protezione dei dati personali dei soggetti interessati residenti nell'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 armonizza le leggi sulla protezione dei dati in tutta Europa e le porta 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 e le organizzazioni che trattano i dati personali dei soggetti interessati residenti in UE sono tenute a rispettare il GDPR.

Dropbox verso la conformità con il GDPR

Dropbox si 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 dei controlli esistenti e offre una serie di iniziative in continua evoluzione per garantire che i dati personali dei nostri utenti siano sempre protetti. 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 passo successivo 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 dei requisiti del GDPR, come ad esempio il mantenimento di registri del trattamento in accordo con l'articolo 30 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.

Responsabilizzare i nostri utenti nell'adozione del GDPR

Dropbox offre funzionalità di controllo e visibilità che possono aiutarti a gestire più facilmente gli obblighi di protezione dei dati, inclusi gli obblighi di conformità al GDPR. Ovviamente, la conformità al 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 al GDPR richiede di pensare in modo più ampio a come i dati si muovono e vengono 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 del 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 Business è uno strumento utile, poiché consente di monitorare l'attività del team, visualizzare i dispositivi connessi e controllare le attività di condivisione. Ci impegniamo per includere i principi Privacy by Design nei nuovi prodotti e nelle nuove funzionalità.

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 Business, puoi gestire facilmente l'accesso dei membri del team a file, cartelle e documenti Paper. Per i collegamenti a file condivisi, la nostra funzionalità 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 funzionalità di cancellazione remota consente di eliminare file e documenti 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 idonei 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.

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, formare i dipendenti sulle pratiche in ambito di sicurezza e privacy, creare una cultura in cui conquistare la fiducia dei clienti 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 svolgono un ruolo fondamentale nella protezione dei propri dati personali. Dropbox ti consente di configurare, utilizzare e monitorare il tuo account in modo da soddisfare le esigenze della tua

organizzazione in merito a privacy, sicurezza e conformità. La nostra guida alla responsabilità condivisa può aiutarti a capire meglio cosa facciamo per mantenere il tuo account al sicuro e cosa puoi fare per garantire 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 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'email all'indirizzo privacy@dropbox.com. Per maggiori informazioni sul GDPR, puoi anche visitare il nostro Centro di orientamento al GDPR.