Dropbox

Sekretess och dataskydd

Introduktion

Personuppgifter spelar en enorm roll i samhället och ekonomin. I allt större utsträckning vill människor ha kontroll och översikt över hur deras personuppgifter används och skyddas av företag de interagerar med.

På Dropbox utgör förtroendet grunden för vårt förhållande med miljontals människor och företag världen över. Vi värdesätter det förtroende du gett oss och tar vårt ansvar att skydda dina personuppgifter på yttersta allvar.

Våra åtaganden gentemot dig

Vi har förbundit oss att skydda dina personuppgifter. Dropbox villkor för tjänsten beskriver ditt ansvar när du använder våra tjänster. Vår integritetspolicy beskriver våra integritetsåtaganden gentemot användare och förklarar hur vi samlar in, använder och hanterar dina personuppgifter när du använder våra tjänster. Om du bor i Nordamerika (USA, Kanada och Mexiko) fungerar Dropbox Inc. som din tjänsteleverantör. För alla andra användare fungerar Dropbox International Unlimited Company som personuppgiftsansvarig för din information.

Om du använder Dropbox Business eller Dropbox Education fungerar din organisation som registeransvarig för personuppgifter som tillhandahålls till Dropbox när du använder Dropbox Business eller Dropbox Education. Den personuppgiftsansvariga avgör syftet och metoderna för behandlingen av personuppgifter.

Dropbox fungerar som personuppgiftsansvarig och behandlar data för din organisations räkning när du använder Dropbox Business eller Dropbox Education, och vårt affärsavtal inkluderar åtaganden relaterade till databehandling och internationella dataöverföringar.

Vårt historiska resultat: efterlevnad

Efterlevnad är ett effektivt sätt att kontrollera en tjänsts trovärdighet. Vi uppmuntrar och gläds över att tillhandahålla oberoende verifiering av att vår säkerhets- och sekretesspraxis uppfyller de mest vedertagna standarderna och förordningarna, som ISO 27001, ISO 27017, ISO 27018, ISO 27701, HIPPA/HITECH samt SOC 1, 2, och 3.

Dessutom var vi en av de första leverantörerna av molntjänster som uppnådde certifiering med ISO 27018, den internationellt erkända standarden för ledande praxis inom molnsekretess och dataskydd. Våra tredjepartsrevisorer testar våra kontroller och tillhandahåller rapporter och utlåtanden. Vi delar dessa med dig när vi har möjlighet. Observera att omfattningen av våra certifikats- och revisionsrapporter vanligtvis avser Dropbox Business och Dropbox Education, men de flesta av våra kontroller gäller också för Dropbox Basic-, Plus- och Professional-användare. Dessutom följer Dropbox nu EU Cloud Code of Conduct. Mer information om de standarder vi efterlever och hur vi verifierar våra rutiner återfinns på vår efterlevnadssida.

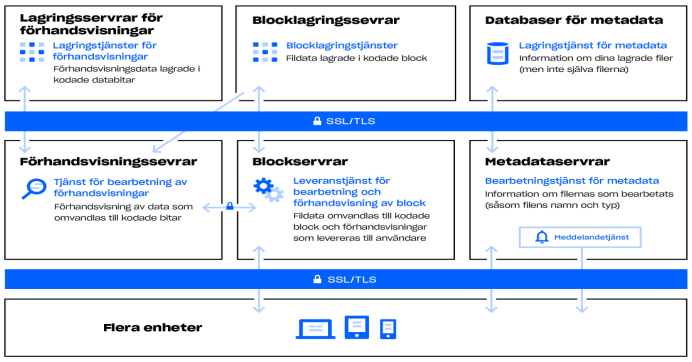
©2023 Dropbox. Med ensamrätt. V2022.08

Dropbox-arkitektur: skydd för dina personuppgifter

På Dropbox tror vi att skyddet av dina personuppgifter utgår från att hålla dina data säkra. Av denna anledning har Dropbox utformats med flera skyddslager som omfattar säker fildataöverföring, kryptering och kontroller på applikationsnivå som distribueras över en skalbar och säker infrastruktur.

Vår infrastruktur: Filer

Dropbox infrastruktur för filer består av de komponenter som visas i diagrammet nedan.



Metadataservrar

Vissa grunduppgifter om användardata, så kallade metadata, lagras i sin egna diskreta lagringstjänst och fungerar som ett index för uppgifterna i användarnas konton. Metadata inkluderar grundläggande konto- och användarinformation som mejladress, namn och enhetsnamn. Metadata innefattar också grundläggande information om filer, inklusive filnamn och typ, vilket underlättar supportfunktioner som versionshistorik, återställning och synkning.

Databaser för metadata

Alla metadata för filer lagras i en MySQL-baserad databastjänst och delas och replikeras efter behov för att leva upp till våra krav på prestanda och hög tillgänglighet.

Blockservrar

Dropbox har designats för att vara en unik säkerhetsmekanism som sträcker sig bortom traditionell kryptering för att skydda användardata. Blockservrar behandlar filer från Dropbox-applikationerna genom att dela upp dem i block. Varje filblock krypteras med starkt chiffer och enbart block som har ändrats mellan granskningarna synkroniseras. När en Dropbox-applikation upptäcker en ny fil eller ändringar i en befintlig fil meddelar applikationen blockservrarna att en ändring genomförts och de nya eller modifierade filblocken bearbetas och överförs till lagringsservrarna.

Blocklagringsservrar

Det faktiska innehållet i användarnas filer lagras i krypterade block på blocklagringsservrarna. Dropbox-klienten delar upp filerna i filblock innan överföringen för att förbereda dem inför lagringen. Lagringsservrarna fungerar som ett CAS-system (Content Adressable Storage), där varje enskilt filblock tas emot baserat på dess hashvärde.

Förhandsvisningsservrar

Förhandsvisningsservrarna ansvarar för att framställa förhandsvisningar av filer. Förhandsvisningar är en framställning av en användares fil i ett annat filformat som är mer lämpat för att snabbt visas på en slutanvändares skärm. Förhandsvisningsservrar hämtar filblock från blocklagringsservrarna för att generera förhandsvisningar. När en förhandsvisning av en fil begärs hämtar förhandsvisningsservrarna den cachelagrade förhandsvisningen från förhandsvisningsservrarna och överför den till blockservrarna. I slutändan levereras förhandsvisningarna till användare via blockservrarna.

Förhandsvisningens lagringsservrar

Cachelagrade förhandsvisningar lagras i ett krypterat format på lagringsservrarna för förhandsvisningar.

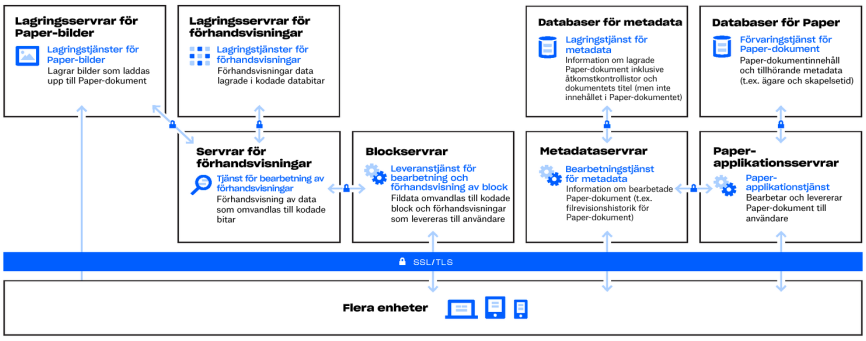
Meddelandetjänst

Denna separata tjänst kontrollerar om några ändringar görs i Dropbox-konton. Inga filer eller metadata lagras eller överförs. Varje klient skapar en long poll-anslutning till meddelandetjänsten och avvaktar. När en fil i Dropbox modifieras signalerar meddelandetjänsten detta till de relevanta klienterna genom att stänga long poll-anslutningen. När anslutningen stängs signalerar detta att klienten måste ansluta till metadatatjänsten på ett säkert sätt för att synkronisera ändringar.

Dropbox

Vår infrastruktur: Paper

Dropbox Paper (Paper) är en funktion i Dropbox-produkten. Paper använder emellertid en distinkt uppsättning system inom Dropbox-infrastrukturmiljön. Papers infrastruktur består av komponenterna som visas i diagrammet nedan.



Paper-applikationsservrar

Paper-applikationsservrar behandlar användarbegäranden, renderar redigerade Paper-dokument tillbaka till användaren och hanterar aviseringstjänster. Paper-applikationsservrar skriver inkommande användarredigeringar till Paper-databaser där de lagras permanent. Kommunikationssessionerna mellan Paper-applikationsservrar och Paper-databaser är krypterade med en stark kod.

Paper-databaser

Det faktiska innehållet i användarnas Paper-dokument, samt vissa metadata om dessa Paper-dokument, lagras permanent i Paper-databaser. Detta omfattar informationen om Paper-dokumentet (som titel, medlemskap och tillstånd som delats, projekt- och mappassociationer och annan information) samt material i själva Paper-dokumentet, inklusive kommentarer och uppgifter. Paper-databaser partitioneras och replikeras efter behov för att uppfylla höga krav på prestanda och tillgänglighet.

Lagringsservrar för Paper-bilder

Bilder som laddas upp till Paper-dokument lagras och krypteras i vila på Paper-bildservrar. Överföringen av bilddata mellan Paper-applikationen och Paper-bildservrar sker över en krypterad session.

Förhandsvisningsservrar

Förhandsvisningsservrar levererar förhandsvisningar av både bilder som laddats upp till Paper-dokument och hyperlänkar som bäddats in i Paper-dokument. För bilder som laddats upp i Paper-dokumentet hämtar förhandsvisningsservrarna bilddata som lagrats i lagringsservrarna för Paper-bilder via en krypterad kanal. För hyperlänkar som bäddats in i Paper-dokument hämtar förhandsvisningsservrarna bilddata och renderar en förhandsvisning av bilden med användning av kryptering i enlighet med källänkens specifikationer. I slutändan levereras förhandsvisningarna till användare via blockservrarna.

Lagringsservrar för förhandsvisningar

Paper använder sig av samma förhandsvisningsservrar som beskrivs i infrastrukturdiagrammet för Dropbox för att lagra cachelagrade förhandsvisningar av bilder. Cachelagrade förhandsvisningar lagras i ett krypterat format på lagringsservrarna för förhandsvisningar.

Dropbox

Dropbox-kontroller: våra interna rutiner

Vi vidtar omfattande åtgärder för att skydda vår infrastruktur, vårt nätverk och våra applikationer. Vissa av åtgärderna vi har på plats inbegriper kryptering i vila, kryptering vid överföring och permanent borttagning av filer. Vi erbjuder också robusta sekretess- och säkerhetsutbildningar för all vår personal för att bygga en kultur där vi prioriterar att förtjäna förtroendet från våra användare. Information om några av våra kontroller ges nedan:

Utbildning

En del av arbetet att skydda våra användares personuppgifter består i att bygga och vårda en kultur av säkerhets- och sekretessmedvetenhet. Dropbox-anställda måste acceptera våra säkerhetspolicyer, inklusive en integritetspolicy för personuppgifter, innan de beviljas systemåtkomst. Endast personal med specifika behov har åtkomst till sådana system. De anställda deltar även i obligatoriska utbildningar i säkerhet och sekretess på årsbasis.

Kryptering under överföring

För att skydda filer under överföring mellan en Dropbox-klient (för närvarande dator, mobil, API eller webb) och Dropbox-frontendservrar skapas en krypterad anslutning som garanterar säker överföring. På liknande vis skapas en krypterad anslutning för att skydda Paper-dokumentdata som överförs mellan en Paper-klient (för närvarande mobil, API eller webb) och värdtjänsten. Dessa anslutningar krypteras med Secure Sockets Layer (SSL)/Transport Layer Security (TLS) vilket skapar en säker tunnel som skyddas av Advanced Encryption Standard-kryptering (AES) som är 128 bitar eller högre.

Kryptering i vila

Filer som laddas upp av användare lagras på Dropbox-lagringsservrar i diskreta filblock. Varje block krypteras med Advanced Encryption Standard (AES) om 256 bitar.

Endast block som modifierats mellan revideringar synkas. På liknande vis krypteras också Paper-dokument som lagras i Dropbox-databaser i vila med 256-bitars Advanced Encryption Standard (AES).

Permanent borttagning av filer och Paper-dokument

När en Dropbox-användare eller en administratör för ett Dropbox Business- eller Dropbox Education-team markerar en fil för permanent radering utlöser detta en process för att permanent radera filen. När en användare eller en administratör för ett Dropbox Business- eller Dropbox Education-team markerar ett Paper-dokument för permanent radering, sker en liknande process för att permanent radera Paper-dokumentdata och bilddata.

Begäran om åtkomst till personuppgifter

För åtkomst till personuppgifter utöver de filer och pappersdokument som lagras i Dropbox kan användare logga in på webbplatsen och gå till sina kontosidor. Kontosidan visar information som namnet och e-postadressen som är kopplad till kontot. Användare kan också se IP-adresserna för anslutna sessioner, datorer och mobila enheter, samt appar som är anslutna till sina konton på säkerhetssidan och sidan för anslutna appar.

Dropbox-användare har också möjlighet att begära åtkomst till eller borttagning av andra personuppgifter Dropbox kan ha samlat in om dem. Mer information om denna process återfinns i Dropbox-hjälpcentret.

Sekretessregelverk på Dropbox

Sekretessteamet ansvarar för att driva Dropbox-sekretessprogrammet. Med det implementerar vi våra viktigaste sekretessinitiativ och arbetar för att bygga in sekretessen i vår datalivscykel. Dropbox sekretessprogram har vidare stöd från flera tvärfunktionella juridiska underteam. Dessa underteam tillhandahåller den vidare expertis som krävs för att driva och övervaka de dagliga uppgifterna i sekretessprogrammet.

DPO-teamet är separerat från de andra sekretessfunktionerna och arbetar i sekretessefterlevnads- och övervakningssyfte i direkt stöd till dataskyddsombudet i utförandet av denna persons uppgifter. Dataskyddsombudet (DPO) kan kontaktas på privacy@dropbox.com.

Dropbox

Principer för dataförfrågningar från myndigheter

Vi förstår att när användare anförtror sina personuppgifter till oss förväntar de sig att vi ska hålla dessa data konfidentiella. Som de flesta andra leverantörer av onlinetjänster får Dropbox ibland förfrågningar från myndigheter som söker information om användare.

I principerna nedan beskriver vi hur vi hanterar databegäranden som vi tar emot från myndigheter.

Var öppen

Vi anser att onlinetjänster ska få publicera antalet och typerna av myndighetsförfrågningar som tas emot, och meddela individer när information om dem har begärts ut. Denna typ av öppenhet ger makt åt användaren eftersom hen på ett bättre sätt kan förstå förekomster och mönster i fråga om myndighetsmissbruk. Vi kommer att fortsätta att publicera detaljerad information om dessa förfrågningar och förespråka rätten att tillhandahålla mer av denna viktiga information.

Kämpa mot alltför omfattande förfrågningar

Myndigheternas dataförfrågningar bör begränsas till informationen de söker och noga skräddarsys för specifika personer och legitima undersökningar. Vi kommer att stå upp mot schablonmässiga eller alltför omfattande förfrågningar.

Tillhandahålla betrodda tjänster

Statliga myndigheter bör aldrig installera bakdörrar i onlinetjänster eller äventyra infrastruktur för att få tag i användardata. Vi kommer att fortsätta skydda våra system och verka för att förändra lagar för att tydliggöra att den här typen av aktivitet är olaglig.

Skydda alla användare

Att ha lagar som ger människor olika skydd beroende på var de bor eller vilket land de är medborgare i är föråldrat och avspeglar inte onlinetjänsternas globala natur. Vi kommer att fortsätta kämpa för en reformering av dessa lagar.

Dessa principer är tillsammans med vår årliga transparensrapport tillgängliga på Dropbox-webbplatsen på adressen: https://www.dropbox.com/transparency.

För ytterligare information om våra kontroller och vår strategi för att skydda dina personuppgifter ska du ta del av vår Dropbox Business-säkerhetssammanställning.

Andra som arbetar för och med Dropbox

Dropbox hanterar de flesta aktiviteter relaterade till tillhandahållandet av våra tjänster, men vi använder vissa betrodda tredjepartsleverantörer med avseende på våra tjänster (till exempel leverantörer av kundsupport och IT-tjänster). Dessa tredje parter kommer endast att få tillgång till din information för att utföra uppgifter för vår räkning i enlighet med vår integritetspolicy och vi behåller fortsatt ansvaret för deras hantering av dina uppgifter i enlighet med våra instruktioner.

Varje tredje part genomgår en noggrann kontrollprocess, inklusive säkerhets- och sekretessgranskningar och regelbundna avtalsgranskningar i syfte att utvärdera deras förmåga att efterleva våra dataskyddsåtaganden. Baserat på denna kontrollprocess bekräftar Dropbox att företagets betrodda tredje parter förbinder sig att följa tillämplig EU-dataskyddslagstiftning i samband med hanteringen av personuppgifter för Dropbox räkning. Kunder kan övervaka betrodda tredjepartsleverantörer till Dropbox genom att granska Dropbox ISO 27001- och 27018-certifieringar och, under lämpliga sekretesskyldigheter, granska Dropbox SOC 2 typ II-rapport. I synnerhet kan kunder övervaka Dropbox betrodda tredje parter genom att granska Dropbox kontroller och revisionsresultat för Trust Services Criteria P6.1, P6.4 och CC.9.2 i SOC 2 typ II-rapporten

Dropbox

Internationella dataöverföringar

När Dropbox överför data från Europeiska unionen, Europeiska ekonomiska samarbetsområdet, Storbritannien och Schweiz, förlitar vi oss på en rad olika rättsliga mekanismer, som till exempel avtal med våra kunder och dotterbolag, standardavtalsklausuler och Europeiska kommissionens lämplighetsbeslut om vissa länder, i tillämpliga fall.

Dropbox följer ramverken för dataskydd mellan EU och USA och Schweiz och USA samt det brittiska tillägget till ramverket för dataskydd mellan EU och USA som fastställts av det amerikanska handelsdepartementet angående behandling av personuppgifter som överförs från EU, Europeiska ekonomiska samarbetsområdet, Storbritannien och Schweiz till USA. Dropbox har certifierat inför det amerikanska handelsdepartementet att det följer dessa ramverk för dataskydd när det gäller sådana uppgifter, men detta inkluderar inte DocSend- eller Formswift-delarna av Tjänsterna.

Du kan läsa mer om ramverket för dataskydd och se Dropbox certifiering på www.dataprivacyframework.gov.

Klagomål och dispyter relaterade till vår efterlevnad av ramverket för dataskydd undersöks och löses genom JAMS, en oberoende tredje part. För mer information kan du läsa vår integritetspolicy.

GDPR: den allmänna dataskyddsförordningen

Den allmänna dataskyddsförordningen, förkortad GDPR, är en EU-förordning som fastställer ett ramverk som skyddar av personuppgifter för registrerade personer i EU. GDPR är den viktigaste nya europeiska dataskyddslagstiftningen sedan EU:s dataskyddsdirektiv från 1995, och många företag – inklusive Dropbox – som har verksamhet i Europa har gjort stora investeringar för att nå GDPR-efterlevnad. GDPR harmoniserar dataskyddslagar i hela Europa och uppdaterar dem i förhållande till den snabba tekniska utveckling som har skett under de senaste två decennierna. Den bygger på befintliga juridiska ramverk i EU, inklusive EU:s dataskyddsdirektiv, och introducerar nya förpliktelser och ansvarsområden för organisationer som hanterar personuppgifter, samt nya rättigheter för individer med avseende på deras personuppgifter. Organisationer som är etablerade i EU, samt organisationer som hanterar personuppgifter för registrerade personer i EU, måste följa GDPR.

Dropbox resa mot GDPR-efterlevnad

Dropbox har ett starkt engagemang för GDPR-efterlevnad. Respekt för sekretess och säkerhet har integrerats i vårt företag från första dagen, och efterhand som vi växt har fokus på att hantera och skydda de data våra användare anförtror oss med fortsatt att vara högprioriterat. Dropbox har en historia av att ligga steget före efterlevnadskurvan – som ovan nämnt var vi en av de första molntjänstleverantörerna att nå ISO 27018-certifiering för våra företagsanvändare. Med utgångspunkt i detta starka fundament ser Dropbox GDPR som en evolution av våra befintliga rutiner och kontroller, och säkerställer en löpande uppsättning initiativ under ständig utveckling för att garantera att våra användares personuppgifter alltid är skyddade. Dropbox-resan mot GDPR-efterlevnad började så fort förordningen beslutades 2016. Vårt första steg var att bilda ett tvärfunktionellt team av dataskyddsspecialister bestående av juridiska ombud, säkerhets- och efterlevnadsexperter och produkt- och infrastrukturutvecklare. Vårt team genomförde sedan en fullständig utvärdering av våra befintliga säkerhets- och dataskyddsrutiner mot GDPR-kraven.

Vårt nästa steg var att genomföra en utvärdering av våra aktiviteter för hantering av personuppgifter, och spåra personuppgifternas livscykel i våra system. Dessa aktiviteter kallas ibland ”datamappning” och att genomföra ”utvärderingar av dataskyddspåverkan”.

Sedan dess har vi fortsatt att bygga på våra befintliga interna processer och procedurer för att säkerställa att vi uppfyller principerna om ansvarsskyldighet i enlighet med GDPR-kraven, inklusive att upprätthålla ett register över vår hantering i enlighet med artikel 30 i GDPR. Detta är viktigt eftersom GDPR lägger ökat fokus på dokumentationsbeslut och -rutiner som påverkar personuppgifter.

Dropbox

Stärka användarna i sina GDPR-resor

Dropbox tillhandahåller funktioner för kontroll och översikt som på ett enklare sätt kan hjälpa er att hantera era dataskyddsåtaganden, inklusive GDPR-efterlevnadskrav. Självklart börjar och slutar inte GDPR-efterlevnad i er organisation med förhållandet till era leverantörer, som Dropbox. Våra funktioner kan hjälpa er att hantera era förpliktelser, men de kan inte i sig själva säkerställa efterlevnad. GDPR-efterlevnad kräver ett större grepp om hur data rör sig och skyddas i er organisation. Varje organisation måste vidta egna åtgärder för att nå efterlevnad, med leverantörer som viktiga partner på denna resa.

Dataminimering

En viktig del av GDPR-kravet på inbyggd sekretess är att organisationer ska konstruera sina tjänster på ett dataminimerande sätt. Detta innebär att ha bra översikt och kontroll över data inom organisationen för att kunna hantera dem. Dropbox Business-adminpanelen är ett användbart verktyg i detta arbete, eftersom panelen hjälper er att övervaka teamaktiviteter, visa anslutna enheter och granska delningsaktiviteter. Vi arbetar för att bygga in sekretess i nya produkter och funktioner.

Skydd och återställning av data

Skydd för borttappade enheter, versionshistorik och filåterställning kan bidra till att skydda mot förluster på grund av olyckor, skador eller förstörelse av personuppgifter, och kan ge möjlighet att återställa tillgängligheten och åtkomsten till personuppgifter på ett smidigt sätt vid en incident. Tvåfaktorautentisering är en annan viktig teknik vi uppmuntrar till, som ett sätt att skydda era data.

Registerhållning

GDPR innebär också ett ökat ansvar för organisationer att föra detaljerade register över sina behandlingsaktiviteter. Våra granskningsloggar och aktivitetsloggar hjälper er att bättre förstå era hanteringsaktiviteter som stöd i ert registerarbete.

Administrationsåtkomst

Inom Dropbox Business-adminpanelen kan du enkelt hantera teammedlemmarnas åtkomst till filer, mappar och Paper-dokument. För delade fillänkar ger vår länkåtkomstfunktion dig möjlighet att lösenordsskydda de delade länkarna, ställa in utgångsdatum för tillfällig åtkomst och begränsa åtkomsten till personer inom din organisation. Om ansvarsområdena skulle ändras mellan användare ger vårt kontoöverföringsverktyg dig möjlighet att enkelt föra över filer och ägarskap av Paper-dokument från en användare till en annan.

Administratörer har också möjlighet att inaktivera en användares åtkomst till användarens konto samtidigt som användarens data och delningsrelationer bevaras i syfte att hålla företagets information säker. Sist men inte minst ger funktionen för fjärradering dig möjlighet att rensa bort filer och Paper-dokument från borttappade eller stulna enheter.

EU-infrastruktur

Även om GDPR inte kräver att personuppgifter ska hanteras inom EU erbjuder Dropbox möjligheten att lagra filer (block) i EU till behöriga Dropbox Business- och Dropbox Education-kunder. EU-baserad fillagring tillhandahålls på Amazon Web Services (AWS) infrastruktur. För mer information om vår EU-infrastruktur ska du kontakta vårt säljteam.

Gemensamt arbete för att skydda dina personuppgifter

Dropbox arbetar med användarna för att skydda deras personuppgifter. Vi vidtar omfattande åtgärder för att skydda vår infrastruktur, vårt nätverk och våra program, utbilda de anställda i rutiner för säkerhet och sekretess, skapa en företagskultur där högsta prioritet är att förtjäna kundernas förtroende och utsätta våra system och rutiner för rigorösa tester och revisioner från tredje part.

Användare spelar emellertid också en nyckelroll för att skydda sina personuppgifter. Dropbox ger dig möjlighet att konfigurera, använda och övervaka ditt konto på sätt som uppfyller din organisations sekretess-, säkerhets- och efterlevnadsbehov. Vår guide om delat ansvar kan hjälpa dig att i större utsträckning förstå vad vi gör för att hålla ditt konto säkert, och vad du kan göra för att bibehålla översikt och kontroll över dina personuppgifter.

Sammanfattning

Varje dag förlitar sig miljontals användare på Dropbox. För att förtjäna detta förtroende har vi byggt och fortsätter att bygga Dropbox med fokus på säkerhet och sekretess. Vårt åtagande för att skydda våra användares personuppgifter ligger till grund för alla beslut vi fattar. För mer information, mejla privacy@dropbox.com. För mer information om GDPR kan du också gå till vårt GDPR- vägledningscenter.