

Sekretess och dataskydd

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 till dig

Vi har förbundit oss att skydda dina personuppgifter. Dropbox [integritetspolicy](#) beskriver våra åtaganden om sekretess och förklarar hur vi samlar in, använder och hanterar dina personuppgifter när du använder våra tjänster. Vi åtar oss även att dela information om våra sekretessrutiner på ett sätt som är lätt att förstå. Vi har tillgängliggjort en [Integritetspolicy: Vanliga frågor](#), samt det här dokumentet för att besvara vanliga frågor.

Bor du i Nordamerika (USA, Kanada och Mexiko) agerar Dropbox, Inc. som din tjänsteleverantör. För alla andra användare agerar Dropbox International Unlimited Company som personuppgiftsansvarig för dina personuppgifter. En personuppgiftsansvarig avgör syftet och metoderna för behandlingen av personuppgifter.

Använder du någon av våra Dropbox för team-planer (till exempel Dropbox Business eller Dropbox Education) fungerar din organisation som personuppgiftsansvarig för alla personuppgifter som tillhandahålls till Dropbox i samband med din användning av Dropbox. I detta fall fungerar Dropbox som personuppgiftsbiträde som behandlar uppgifter för din organisations räkning i enlighet med vårt [Business-avtal](#), där vi beskriver våra åtaganden relaterat till personuppgiftsbehandling och internationell dataöverföring.

Oavsett din plan använder Dropbox samma principer när det gäller hanteringen av dina personuppgifter. Följande avsnitt beskriver våra företagsprinciper och ger en inblick i hur vi efterlever globala certifieringar och sekretessföreskrifter.



Principer för dataförfrågningar från statliga myndigheter

Vi förstår att när användare anförtror sina personuppgifter till oss förväntar de sig att vi ska hålla dessa data konfidentiella. Precis som de flesta andra onlinetjänster får Dropbox ibland förfrågningar från polis och andra myndigheter som vill ha information om våra användare. Vi granskar varje förfrågan och åtar oss att i enlighet med lag meddela användare när deras konton identifieras i en förfrågan.

Vi upprätthåller en insynsrapport och har upprättat följande principer för dataförfrågningar från statliga myndigheter:

Var öppen

Onlinetjänster bör få publicera det antal och typ av myndighetsförfrågningar de får in och meddela enskilda personer när det finns en informationsförfrågan om dem. 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.

Bekämpa överdrivet icke-specifika 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.

Tillhandahåll tillförlitliga tjänster

Myndigheter ska aldrig kunna 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.

Dessa principer, tillsammans med vår årliga insynsrapport, finns tillgängliga på Dropbox webbplats: [Dropbox insynsöversikt](#).

Principer för artificiell intelligens

Vissa av Dropbox funktioner drivs av artificiell intelligens (AI). Dropbox arbetar för att se till att våra AI-innovationer inte bara hjälper våra kunder utan också respekterar deras rättigheter och säkerhet.

Följande principer vägleder våra team i takt med att vi utvecklar AI-produkter och -funktioner på ett ansvarsfullt sätt:

- Utnyttja AI för att betjäna våra kunder
- Säkerställa att kunderna har kontroll över sina data
- Vara öppna med hur vi använder AI
- Främja rättvis teknik inom AI
- Hållas ansvariga inför våra kunder
- Respektera människor och deras säkerhet och rättigheter

Dessa principer beskrivs mer ingående på Dropbox webbplats: [Dropbox AI-principer](#).



Dropbox-kontroller: våra interna metoder

Vi vidtar omfattande åtgärder för att skydda vår infrastruktur, vårt nätverk och våra applikationer. Några av de säkerhetsåtgärder vi har infört är kryptering i vila, kryptering vid överföring och åtkomstkontroller. Dessa åtgärder beskrivs i detalj i [Dropbox vitbok om säkerhet](#).

Våra robusta säkerhetskontroller kompletteras av en uppsättning sekretesskontroller. Några exempel är:



Sekretessutbildning

En del av arbetet att skydda våra användares personuppgifter består i att bygga och vårda en kultur av sekretessmedvetenhet. Dropbox medarbetare måste godkänna en data integritetspolicy som gäller användaruppgifter och en policy för hemligstämpling av data innan de får åtkomst till systemet. Endast personal med specifika behov har åtkomst till sådana system. Medarbetare deltar även i en obligatorisk sekretessutbildning varje år. Dessa utbildningar lär ut grunderna i sekretesslagar och beskriver bästa praxis gällande hantering av personuppgifter på Dropbox.



Permanent radering av filer och Paper-dokument

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



Anonymisering och pseudonymisering

I vissa fall där vi inte längre behöver uppgifter som kan hänföras till en person, använder vi metoder som anonymisering och pseudonymisering för att avidentifiera uppgifterna. Anonymisering tar bort eller ändrar personuppgifter permanent så att de inte kan användas för att identifiera en individ. Pseudonymisering tar tillfälligt bort eller ändrar personuppgifter, men processen kan vändas om någon har åtkomst till ytterligare information. Ett exempel på när vi använder pseudonymisering är när vi avidentifierar kundfeedback och använder den för att förbättra våra produkter och tjänster.



Sekretesstyrning

Sekretessteamet ansvarar för att driva Dropbox sekretessprogram. Det implementerar våra viktiga sekretessinitiativ och förespråkar inbyggd sekretess i vår datalivscykel. Dropbox sekretessprogram stöds ytterligare av flera tvärfunktionella delteam på juridik- och säkerhetsavdelningarna. Dessa delteam tillhandahåller den extra expertis som krävs för att driva och övervaka sekretessprogrammets dagliga uppgifter.

Dataskyddsombudets kansli arbetar åtskilt från övriga sekretessteam och har en sekretessfunktion för efterlevnad och tillsyn. De kan kontaktas via privacy@dropbox.com.

Våra meriter: 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, SOC 1, SOC 2 och SOC 3**.

Vi är stolta över att ha varit bland de första molntjänsteleverantörerna att bli certifierade för ISO 27018, den internationellt erkända standarden för ledande rutiner inom molnsekretess och dataskydd. Våra tredjepartsrevisorer testar våra kontroller och tillhandahåller rapporter och utlåtanden. Vi delar dessa med er när vi har möjlighet. Observera att även om omfattningen av våra certifieringar och revisionsrapporter vanligtvis hänvisar till Dropbox för team, är majoriteten av våra kontroller tillämpliga på alla Dropbox-planer.

Dessutom följer Dropbox **EU:s uppförandekod för molntjänster**. EU:s uppförandekod för molntjänster är ett frivilligt instrument som gör det möjligt för en molntjänstleverantör, till exempel Dropbox, att visa sitt engagemang för efterlevnad av dataskyddslagen. Dropbox för team har förklarats följa EU:s uppförandekod för molntjänster och har tilldelats efterlevnadsmärket på "nivå 2", vilket innebär att dessa tjänster har implementerat tekniska, organisatoriska och avtalsrelaterade åtgärder i enlighet med uppförandekodens krav. Mer information finns på [kodens officiella webbplats](#).

Mer information om de standarder som vi följer och hur vi verifierar våra metoder finns i vårt [Trust Center](#) och vår [webbplats för efterlevnad](#).

Internationell överföring av data

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.

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 Formswift-delen av tjänsterna.

Du kan läsa mer om ramverket för dataskydd och se Dropbox certifiering på <https://www.dataprivacyframework.gov/>.

Klagomål och tvister relaterade till vår efterlevnad av ramverket för dataskydd undersöks och löses genom JAMS, en oberoende tredje part. Mer information hittar du i vår [integritetspolicy](#).

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 granskningar av säkerhet, sekretess och avtal, 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 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. Med lämpliga sekretesskrav kan en kund också övervaka Dropbox betrodda tredje parter genom att undersöka Dropbox resultat för kontroll och granskning av kriterierna för betrodda tjänster P6.1, P6.4 och CC.9.2 i SOC 2 Typ II-rapport.

Dessutom kan Dropbox anlita underbiträden med åtkomst till kundernas personuppgifter i syfte att aktivera etableringen av tjänster. Innan vi anlitar underbiträden, genomför Dropbox en granskning av underleverantörernas rutiner för sekretess, säkerhet och konfidentialitet, och vidtar lämpliga avtalsåtgärder avseende skydd av personuppgifter. Du kan se listan över underbiträden och registrera dig för ändringar av underbiträden genom att besöka vår [lista över underbiträden](#).

Den allmänna dataskyddsförordningen

Den allmänna dataskyddsförordningen, förkortad GDPR, är en EU-förordning som fastställer ett ramverk som skyddar personuppgifter för registrerade personer i EU. GDPR är den viktigaste nya europeiska dataskyddslagstiftningen sedan EU:s dataskyddsdirektiv från 1995, och företag – inklusive Dropbox – som har verksamhet i Europa har gjort stora investeringar för att nå GDPR-efterlevnad.

Respekt för sekretess och säkerhet har integrerats i vårt företag från dag ett, och i takt med vår tillväxt 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 nämndes ovan var vi en av de första molntjänstleverantörerna att nå ISO 27018-certifiering för våra företagsanvändare. Med tanke på denna starka grund var GDPR-efterlevnaden en naturlig utveckling av våra befintliga rutiner och kontroller.

Dropbox resa mot GDPR-efterlevnad började så snart förordningen antogs 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.

Mer information om GDPR hittar du i vårt [GDPR-vägledningscentrum](#).



Registrerades rättigheter

GDPR ger enskilda personer rätten att få tillgång till, korrigera, radera och invända mot behandling av deras personuppgifter. Dessa konsumenträttigheter återfinns även i ett antal andra sekretesslagar, såsom California Consumer Privacy Act (CCPA). Så här följer Dropbox dessa sekretessrättigheter:



Rätt till åtkomst och korrigerings

Användare kan komma åt eller korrigera uppgifter om sig själva genom att logga in på <https://www.dropbox.com> och gå till sin kontosida. [Fliken "Allmänt"](#) visar information som namn och mejladress som är kopplade till kontot. [Fliken "Säkerhet"](#) visar IP-adresserna för anslutna sessioner, datorer och mobilenheter, medan [Fliken "Appar"](#) visar de appar som är kopplade till kontot.

Dropbox har också lanserat en ["Sekretess"-flik](#), där användare kan skapa åtkomstrapporter. Personer som inte kan logga in på sitt konto eller som inte har ett, kan skicka en begäran om dataåtkomst genom att fylla i detta formulär: [formulär för begäran om registrerade personuppgifter](#).



Rätt att radera

Användare som vill radera sitt kontoinnehåll kan göra det direkt från sina konton. Mer information om hur du raderar innehåll [finns här](#).

Användare kan gå till fliken "Sekretess" för att radera icke-kontorelaterade uppgifter (till exempel kontaktinformation i våra marknadsföringssystem). Personer som inte kan logga in på sitt konto eller som inte har ett konto kan skicka en begäran om radering genom att fylla i detta formulär: [formulär för begäran om registrerade personuppgifter](#).



Rätt att invända

Beroende på vilken behandling det rör sig om kan individer begära att vi avbryter eller begränsar behandlingen av deras personuppgifter. Om du vill invända mot behandlingen av dina personuppgifter, ber vi dig att mejla oss på privacy@dropbox.com.

Personer kan när som helst välja bort marknadsföringsmaterial genom att ändra sina preferenser i avsnittet [meddelanden](#) på sitt konto, eller genom att klicka på länken för "avsluta prenumeration" i sidfoten på marknadsföringsmejl.

Personer kan också välja bort insamling av personuppgifter med kakor genom att uppdatera sina preferenser i Dropbox kakkbanner. Mer information om Dropbox användning av kakor och liknande teknik finns på [den här sidan](#).

Vi ger våra användare resurser

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. Adminpanelen för Dropbox för team 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 och komma åt personuppgifter på ett smidigt sätt vid en incident. Tvåfaktorautentisering är en annan viktig teknik vi uppmuntrar som ett sätt att skydda era data.



Registerhållning

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



Administrationsåtkomst

I adminpanelen för Dropbox för team kan ni enkelt hantera teammedlemmarnas åtkomst till filer, mappar och Paper-dokument. När det gäller delade fillänkar, låter vår funktion för länkbehörighet er lösenordsskydda de delade länkarna, ställa in utgångsdatum för tillfällig åtkomst och begränsa åtkomsten till personer inom er organisation. I händelse att ansvarsområdena ändras mellan användare, kan ni enkelt föra över filer och ägarskap av Paper-dokument från en användare till en annan med vårt kontoöverföringsverktyg. Administratörer har också möjlighet att inaktivera en användares åtkomst till sitt konto samtidigt som användarens data och delningsrelation bevaras i syfte att hålla er organisations information säker. Sist men inte minst ger funktionen för fjärradering er 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 för team-kunder. Om du vill ha mer information om vår EU-infrastruktur kan du [kontakta vårt säljteam](#).

Vi arbetar tillsammans 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. För att åstadkomma detta utbildar vi de anställda i rutiner för säkerhet och sekretess, skapar en företagskultur där högsta prioritet är att förtjäna kundernas förtroende samt genom att låta våra system och rutiner genomgå rigorösa tester och granskningar av tredje part.

Men användare spelar också en viktig roll när det gäller att skydda sina personuppgifter. Dropbox [användarvillkor](#) beskriver ditt ansvar när du använder våra tjänster. Dropbox gör att du kan konfigurera, använda och övervaka ditt konto på ett sätt som tillgodoser din organisations sekretess-, säkerhets- och efterlevnadsbehov. Vår [guide om delat ansvar](#) kan hjälpa dig att bättre förstå vad vi gör för att skydda ditt konto och vad du kan göra för att upprätthålla synlighet och kontroll över dina personuppgifter.

Om du vill ha mer information om innehållet i detta dokument, kan du skicka e-post till privacy@dropbox.com.

