

Beskyttelse af personlige oplysninger og data

Indledning

Personoplysninger spiller en stor rolle i samfundet og økonomien. Folk søger i stigende grad større kontrol og klarhed om, hvordan deres personlige data bruges og beskyttes af organisationer, de interagerer med.

Hos Dropbox udgør tillid grundlaget for vores relation med millioner af mennesker og virksomheder rundt om i verden. Vi værdsætter den tillid, du har vist os, og tager ansvar for at beskytte dine personlige data alvorligt.

Vores forpligtelser over for dig

Vi forpligter os til at beskytte dine personlige data. Dropbox' [Servicebetingelser](#) beskriver dine forpligtelser, når du bruger vores tjenester.

Vores [politik til beskyttelse af personlige oplysninger](#) beskriver vores forpligtelser over for brugerne om beskyttelse af personlige oplysninger og forklarer, hvordan vi indsamler, bruger og håndterer dine personlige data, når du bruger vores tjenester. Hvis du bor i Nordamerika (USA, Canada og Mexico) fungerer Dropbox Inc. som din tjenesteudbyder. For alle andre

brugere fungerer Dropbox International Unlimited Company som en dataansvarlig for dine personlige data.

Hvis du bruger Dropbox Business eller Dropbox Education, fungerer din organisation som den dataansvarlige for evt. personlige data, der leveres til Dropbox i forbindelse med din brug af Dropbox Business eller Dropbox Education. Den dataansvarlige bestemmer formål og midler til behandling af personoplysninger.

Dropbox fungerer som databehandler, og behandler data på din organisations vegne, når du bruger Dropbox Business eller Dropbox Education, og vores [virksomhedsaftale](#) inkluderer forpligtelser relateret til databehandling og international dataoverførsel.

Vores historie: Overholdelse af regler

Overholdelse af regler er en effektiv måde at validere en tjenestes troværdighed på. Vi opfordrer til og leverer gerne uafhængig verificering af, at vores praksis for sikkerhed og beskyttelse af personlige oplysninger overholder de mest accepterede standarder og lovgivninger som ISO 27001, ISO 27018, HIPPA / HITECH, den tyske BSI C5 og SOC 1, 2 og 3. Desuden var vi en af de første cloud-tjenesteudbydere, der opnåede certificering med ISO 27018, den

internationalt anerkendte standard for førende praksis inden for cloudbaseret beskyttelse af personlige oplysninger og data. Vores uafhængige tredjeparts revisorer tester vores kontrolforanstaltninger og leverer deres rapporter og meninger. Vi deler disse med dig, når det er muligt.

Bemærk, at mens omfanget af vores certificeringer og revisionsrapporter typisk henviser til Dropbox Business og Dropbox Education, er størstedelen af

vores kontroller også gældende for brugere af Dropbox Basic, Plus og Professional. Derudover overholder Dropbox nu CSA's adfærdskodeks for overholdelse af GDPR.

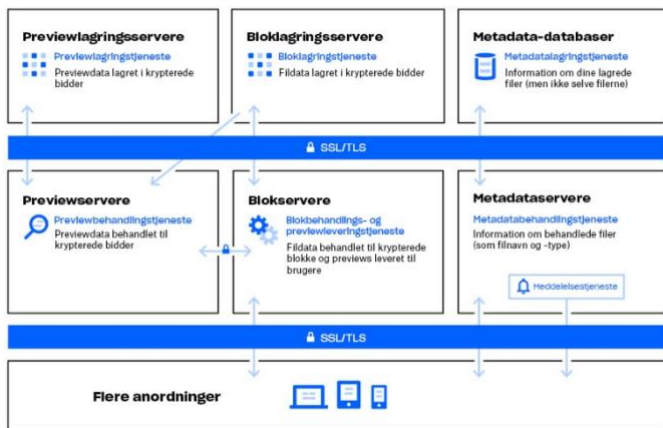
Flere oplysninger om de standarder, som vi overholder, og hvordan vi verificerer vores praksis, kan findes på vores webside om overholdelse.

Dropbox' arkitektur: Beskyttelse af dine personlige data

Hos Dropbox er det vores opfattelse, at beskyttelse af dine personlige data skal tage udgangspunkt i at holde dine data sikre. Dropbox er derfor udviklet med adskillige beskyttelseslag, inklusive sikker overførsel af fildata, kryptering og kontrolforanstaltninger på applikationsniveau fordelt på en skalerbar og sikker infrastruktur.

Vores infrastruktur: Servere for filmetadata

Dropbox' infrastruktur for filer består af de komponenter, som er vist i nedenstående diagram.



Bloklagerservere

Det faktiske indhold af brugernes filer lagres i krypterede blokke på bloklagerserverne. Før overførslen opdeler Dropbox-klienten filerne i filblokke som forberedelse til lagringen. Bloklagerserverne fungerer som et CAS-system (Content-Addressable Storage), hvor hver enkelt krypteret filblok hentes på baggrund af dens hash-værdi.

Previewservere

Previewserverne er ansvarlige for at producere previews af filer. Previews er en gengivelse af en brugers fil i et andet filformat, der er bedre egnet til hurtig visning på en slutbrugers anordning. Previewservere henter filblokke fra bloklagerserverne for at generere previews. Når der anmodes om et filpreview, henter previewserverne det cachede preview fra previewlagerserverne og overfører det til blokserverne. Til sidst vises previewet for brugere af blokserverne.

Previewlagerservere

Cachede previews lagres i et krypteret format på previewlagerserverne.

Meddelelsetjeneste

Formålet med denne separate tjeneste er at overvåge, om der foretages nogen ændringer til Dropbox-konti. Ingen filer eller metadata opbevares eller overføres her. Hver klient etablerer en lang forespørgselsforbindelse til meddelelsetjenesten og venter. Når der sker en ændring til en fil i Dropbox, giver meddelelsetjenesten besked om ændringen til den eller de pågældende klient(er) ved at lukke den lange forespørgselsforbindelse. Når forbindelsen lukkes, er det tegn på, at klienten skal oprette en sikker forbindelse til metadataserverne for at synkronisere eventuelle ændringer.

Metadataservere

Visse grundlæggende oplysninger om brugerdata, der kaldes metadata, opbevares i deres egen særskilte lagertjeneste og fungerer som et indeks for dataene på brugernes konti. Metadataene indeholder grundlæggende konto- og brugeroplysninger, f.eks. e-mailadresse, navn og enhedsnavne. Metadataene indeholder også grundlæggende oplysninger om filer, f.eks. filnavne og -typer, der understøtter funktioner som versionshistorik, gendannelse og synkronisering.

Metadata-databaser

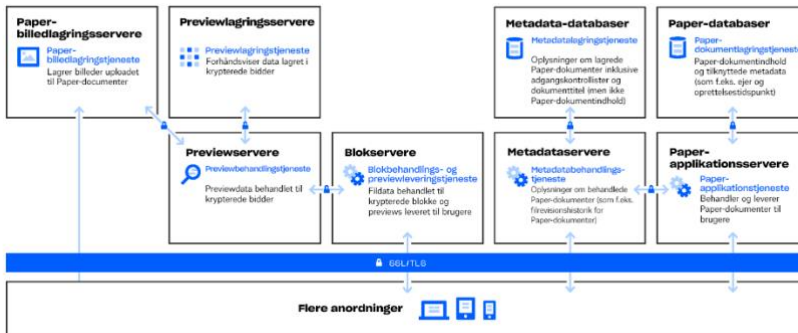
Filmetadata lagres i en MySQL-baseret databasetjeneste og deles og kopieres efter behov for at opfylde kravene til ydeevne og høj tilgængelighed.

Blokservere

Dropbox er designet med en unik sikkerhedsmekanisme, som beskytter brugerdata med mere end blot traditionel kryptering. Blokservere beskytter filer fra Dropbox-applikationerne ved at opdele hver fil i blokke, kryptere hver enkelt filblok ved hjælp af en stærk kode og kun synkronisere de blokke, som er ændret mellem revisioner. Når en Dropbox-applikation registrerer en ny fil eller ændringer til en eksisterende fil, giver applikationen besked om ændringen til blokserverne, og nye eller ændrede filblokke behandles og overføres til lagerserveren.

Vores infrastruktur: Paper

Dropbox Paper (Paper) er en funktion i Dropbox-produktet. Men Paper benytter et separat sæt af systemer i Dropbox-infrastrukturen. Papers infrastruktur består af de komponenter, der er vist i nedenstående diagram.



Paper-applikationsservere

Paper-applikationsserverne behandler brugeranmodninger, viser output af redigerede Paper-dokumenter tilbage til brugeren og kører meddelelsestjenester. Paper-applikationsservere skriver indgående brugerændringer til Paper-databaserne, hvor de gemmes i permanent lager. Kommunikationssessioner mellem Paper-applikationsserverne og Paper-databaserne er krypteret vha. en stærk krypteringsalgoritme.

Paper-databaser

Det faktiske indhold af brugernes Paper-dokumenter samt visse metadata om Paper-dokumenter krypteres i permanent lager i Paper-databaserne. Dette inkluderer oplysninger om et Paper-dokument (f.eks. titlen, delt medlemskab og delte tilladelser, projekt- og mappetilknævninger og andre oplysninger) samt indholdet i selve Paper-dokumentet, herunder kommentarer og opgaver. Paper-databaserne opdeles og kopieres efter behov for at opfylde kravene til ydeevne og høj tilgængelighed.

Paper-billedlagerservere

Billeder, der uploades til Paper-dokumenter, gemmes og krypteres i hvile på Paper-billedserverne. Overførsel af billeddata mellem Paper-applikationen og Paper-billedserverne foregår via en krypteret session.

Previewservere

Previewserverne producerer previews for både billeder, som uploades til Paper-dokumenter, og for hyperlinks, som er indlejret i Paper-dokumenter. For billeder, der uploades til Paper-dokumenter, henter previewserverne billeddata, der er lagret på Paper-billedlagerserverne, gennem en krypteret kanal. For hyperlinks, der er indlejret i Paper-dokumenter, henter previewservere billeddataene og viser et preview af billedet ved hjælp af kryptering, der er specificeret i kodelinket. Til sidst vises previewet for brugere af blokservere.

Previewlagerservere

Paper bruger de samme previewlagerservere, der er beskrevet i diagrammet over Dropbox-infrastrukturen, til at lagre cachede billedpreviews. Bidder af cachede previews lagres i et krypteret format på previewlagerserverne.

Dropbox-kontrolelementer: Vores interne praksis

Vi træffer omfattende foranstaltninger for at beskytte vores infrastruktur, netværk og applikationer. Nogle af de sikkerhedsforanstaltninger, vi har på plads, inkluderer kryptering i hvile, kryptering under overførsel og permanent sletning af filer. Vi tilbyder også grundig uddannelse i sikkerhed og beskyttelse af personlige oplysninger for alle vores medarbejdere for at opbygge en kultur, hvor pålidelighed er en prioritet. Nedenfor beskrives vores kontrolforanstaltninger i detaljer:

Oplæring

En del af beskyttelsen af vores brugeres personlige data består i at opbygge og fremme en kultur med opmærksomhed på sikkerhed og beskyttelse af personlige oplysninger. Dropbox' medarbejdere skal acceptere sikkerhedspolitikker, herunder en politik for beskyttelse af brugernes personlige data, før de får adgang til systemerne. Kun medarbejdere med et specifikt behov har adgang til sådanne systemer. Medarbejdere deltager også i obligatorisk uddannelse i sikkerhed og beskyttelse af personlige oplysninger på årsbasis.

Kryptering under overførsel

For at beskytte fildata under overførsel mellem en Dropbox-klient (i øjeblikket computer, mobil, API eller web) og Dropbox' frontend-servere etableres der en krypteret forbindelse for at sørge for sikker levering. På samme måde etableres der en krypteret forbindelse for at beskytte Paper-dokumentdata under overførsel mellem en Paper-klient (i øjeblikket mobil, API eller web) og værtstjenesten. Disse forbindelser krypteres vha. Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for at oprette en sikker tunnel, der er beskyttet ved hjælp af 128-bit eller bedre Advanced Encryption Standard-kryptering (AES).

Kryptering i hvile

Filer, som brugerne uploader, bliver gemt på Dropbox' lagere servere som separate filblokke. Hver blok krypteres ved hjælp af 256-bit Advanced Encryption Standard (AES).

Kun de blokke, der er blevet ændret mellem versioner, synkroniseres. På samme måde krypteres Paper-dokumentdata i hvile, som er gemt i Paper-databaser, ved hjælp af 256-bit Advanced Encryption Standard (AES).

Permanent sletning af filer og Paper-dokumenter

Når en hvilken som helst bruger af Dropbox eller administrator for Dropbox Business- eller Dropbox Education-team markerer en fil til permanent sletning, udløser det en proces for at slette filen permanent.

Når en bruger eller en administrator for et Dropbox Business- eller Dropbox Education-team markerer et Paper-dokument til permanent sletning, findes der på samme måde en lignende proces til at slette Paper-dokumentdata og -billeddata permanent.

Anmodninger om adgang til personlige data

For at få adgang til personlige data ud over de filer og papirdokumenter, der er gemt i Dropbox, kan brugerne logge ind på webstedet og gå til deres [kontoside](#). Kontosiden viser oplysninger som f.eks. det navn og e-mailadresse, der er knyttet til kontoen. Brugere kan også se IP-adresser for tilsluttede sessioner, computere og mobile enheder samt apps, der er forbundet til deres konti fra [sikkerhedssiden](#) og [siden med tilsluttede apps](#).

Dropbox-brugere har også mulighed for at anmode om adgang til eller sletning af andre personlige data, som Dropbox muligvis har indsamlet om dem.

Flere oplysninger om denne proces kan findes i Dropbox [Hjælp Center](#).

Forvaltning af persondata hos Dropbox

Teamet for beskyttelse af persondata er ansvarlig for driften af Dropbox's persondataprogram. Det implementerer vores vigtigste initiativer omkring beskyttelse af persondata og kæmper for databeskyttelse som design ("Privacy By Design") i vores datalivscyklus. Dropbox' persondataprogram understøttes yderligere af flere tværfunktionelle juridiske underordnede teams. Disse underordnede teams giver den ekstra ekspertise, der kræves til at drive og overvåge de daglige opgaver i persondataprogrammet. T

DPO-teamet fungerer adskilt fra de andre funktioner til beskyttelse af persondata og fungerer direkte som overholdelse af og tilsyn med beskyttelse af persondata, som støtte af den databeskyttelsesansvarlige i udførelsen af deres opgaver. Den databeskyttelsesansvarlige (DPO) kan kontaktes på privacy@dropbox.com.



Principper for myndighedernes anmodning om data

Vi er klar over, at når brugerne betror os deres personlige data, forventer de, at vi holder dataene fortrolige. Som det er tilfældet for de fleste onlinetjenester, modtager Dropbox undertiden anmodninger fra myndigheder, der søger oplysninger om deres brugere.

Nedenstående principper beskriver, hvordan vi håndterer de dataanmodninger, som vi modtager fra myndighederne.

Være åbne

Vi er af den opfattelse, at onlinetjenester skal have tilladelse til at offentliggøre antallet og arterne af de anmodninger, de modtager fra myndighederne, og at give enkeltpersoner besked, når der anmodes om oplysninger om dem. Denne form for åbenhed styrker brugerne ved at give dem

bedre viden om tilfælde og mønstre i myndighedskontrol. Vi vil fortsat offentliggøre detaljerede oplysninger om disse anmodninger og tale for retten til at levere flere af disse vigtige oplysninger.

Bestrid for brede anmodninger

Myndighedernes dataanmodninger bør være begrænset i, hvilke oplysninger de ønsker, og begrænset til bestemte personer og legitime undersøgelser. Vi vil bestride generelle og for brede anmodninger.

Tilbyd troværdige tjenester

Myndigheder bør aldrig installere bagdøre til onlinetjenester eller kompromittere infrastrukturen for at skaffe brugerdata. Vi kæmper fortsat for at beskytte vores systemer og ændre lovene for at gøre det klart, at denne type aktivitet er ulovlig.

Beskytte alle brugere

Love, der giver mennesker forskellig beskyttelse, afhængigt af hvor de bor eller deres statsborgerskab, er forældede og afspejler ikke onlinetjenesters globale natur. Vi vil fortsætte med at tale for ændringer af sådanne love.

Disse principper samt vores årlige gennemsigtighedsrapport gøres offentligt tilgængelige på webstedet for Dropbox på:

<https://www.dropbox.com/transparency>.

Du kan få flere oplysninger om vores kontrolforanstaltninger og vores fremgangsmåder til at beskytte dine personlige data ved at besøge vores [Hvidbog om sikkerhed i Dropbox Business](#).

Andre, som arbejder for og med Dropbox

Dropbox administrerer størstedelen af aktiviteter relateret til levering af vores tjenester; dog bruger vi nogle pålidelige tredjeparter i forhold til vores tjenester (for eksempel udbydere af kundesupport og it-tjenester).

Disse tredjeparter har kun adgang til dine oplysninger for at udføre opgaver på vores vegne i overensstemmelse med vores [politik til beskyttelse af personlige oplysninger](#), og vi forbliver ansvarlige for deres håndtering af dine oplysninger i overensstemmelse med vores instruktioner.

Hver tredjepart gennemgår en streng kontrolproces, herunder gennemgang af sikkerhed og politikker til beskyttelse af personlige oplysninger samt regelmæssige kontraktlige gennemgange for at evaluere deres evne til at opfylde vores forpligtelser til databeskyttelse.

Baseret på denne kontrolproces bekræfter Dropbox, at dets betroede tredjeparter forpligter sig til at overholde gældende EU's databeskyttelseslovgivning i forbindelse med behandling af personoplysninger på Dropbox's vegne.

Kunder kan overvåge Dropbox' betroede tredjeparter ved at gennemgå Dropbox's ISO 27001- og 27018-certificeringer og under passende fortrolighedsforpligtelser gennemgå Dropbox's SOC 2 Type II-rapport. Især kan kunder overvåge Dropbox's betroede tredjeparter ved at undersøge Dropbox's kontroller og revisionsresultater for Trust Services Criteria P6.1, P6.4 og CC . 9.2 i SOC 2 Type II-rapporten.

Internationale dataoverførsler

Ved overførsel af data fra EU, Det Europæiske Økonomiske Samarbejdsområde og Schweiz er Dropbox afhængig af en række juridiske mekanismer såsom kontrakter med vores kunder og tilknyttede selskaber, standardkontraktbestemmelser og Europa-Kommissionens beslutninger om et tilstrækkeligt beskyttelsesniveau for visse lande, alt efter hvad der er relevant.

Dropbox overholder rammerne for EU's og USA's privatlivsskjold og Schweiz' og

USA's privatlivsskjold som beskrevet af US Department of Commerce vedrørende indsamling, brug og opbevaring af personoplysninger, der overføres fra EU, Det Europæiske Økonomiske Samarbejdsområde, Storbritannien og Schweiz til USA, selvom Dropbox ikke forlader sig på rammerne for EU's og USA's privatlivsskjold eller Schweiz' og USA's privatlivsskjold som et juridisk grundlag for overførsel af

personoplysninger. Du kan finde dropbox' privatlivsskjoldscertificering www.privacyshield.gov/list. Du kan også lære mere om privatlivsskjold på www.privacyshield.gov.

Klager og tvister i relation til vores Privacy Shield-overholdelse undersøges og løses gennem JAMS, en uafhængig tredjepart. Du kan finde flere oplysninger i vores [politik for beskyttelse af personlige oplysninger](#).

GDPR: Den generelle forordning om databeskyttelse

Den generelle forordning om databeskyttelse, også kaldet GDPR, er et EU-regulativ, der skaber et nyt juridisk grundlag for beskyttelse af EU-borgeres personlige data.

GDPR er den mest betydningsfulde europæiske lovgivning vedrørende databeskyttelse siden EU's databeskyttelsesdirektiv fra 1995, og mange virksomheder – herunder Dropbox – der driver forretning i Europa, har investeret mange penge i overholdelse af GDPR.

GDPR harmoniserer databeskyttelseslovgivning overalt i Europa og opdaterer dem, så de svarer til den hurtige teknologiske ændring, der er sket i de sidste to årtier.

Den er baseret på tidligere juridiske regler i EU, herunder EU's databeskyttelsesdirektiv, og introducerer nye forpligtelser og ansvarsområder for organisationer, der håndterer personlige

data samt nye rettigheder for enkeltpersoner med hensyn til deres personlige data. Organisationer, der er etableret i EU, såvel som organisationer, der behandler personoplysninger om EU-registrerede, skal overholde GDPR.

Dropbox' bestræbelser for at overholde GDPR

Dropbox er forpligtet til at overholde GDPR. Respekt for beskyttelse af persondata og sikkerhed har fra starten af været en integreret del af vores forretning, og efterhånden som vi er vokset, har fokus på håndtering og beskyttelse af de data, som brugerne betror os, til stadighed haft høj prioritet. Dropbox har altid holdt sig forrest mht. overholdelse – som beskrevet ovenfor var vi en af de første udbydere af cloudtjenester, der opnåede ISO 27018-certificering for vores erhvervsbrugere. Med dette stærke fundament anser Dropbox overholdelse af GDPR som en videreudvikling af vores eksisterende praksisser og kontrolforanstaltninger, og repræsenterer et løbende, udviklende sæt initiativer for at sikre, at vores brugeres personlige data altid er beskyttet.

Dropbox' bestræbelser for at overholde GDPR begyndte, i det øjeblik forordningen blev vedtaget i 2016. Vores første skridt var at danne et tværfunktionelt team af databeskyttelseseksperter bestående af juridiske rådgivere, specialister inden for sikkerhed og overholdelse samt produkt- og infrastrukturudviklere. Vores team udarbejdede derefter en komplet vurdering af vores aktuelle arbejdsgange for sikkerhed og databeskyttelse i forhold til kravene i GDPR.

Vores næste skridt var at evaluere vores aktiviteter til behandling af persondata og spore persondataenes livscyklus i vores systemer. Disse øvelser kaldes undertiden udførelse af datatilknytninger og gennemførelse af konsekvensanalyser af databeskyttelse.

Sidenhen er vi fortsat med at bygge videre på vores eksisterende interne processer og procedurer for at sikre, at vi lever op til ansvarlighedsprincipperne i henhold til kravene i GDPR, herunder vedligeholdelse af fortegnelser over behandling i overensstemmelse med artikel 30 i GDPR. Dette er vigtigt, eftersom GDPR sætter ekstra fokus på at dokumentere beslutninger og fremgangsmåder, der påvirker persondata.

Styrkelse af vores brugere i deres GDPR-bestræbelser

Dropbox leverer funktioner til kontrol og gennemsigtighed, som kan hjælpe dig med lettere at håndtere dine databeskyttelsesforpligtelser, herunder forpligtelser til at overholde GDPR. Det siger sig selv, at overholdelse af GDPR i din organisation hverken begynder eller slutter med dine leverandører som f.eks. Dropbox. Vores funktioner kan hjælpe dig med at administrere dine forpligtelser, men de kan ikke i sig selv sikre overholdelse. Overholdelse af GDPR kræver, at du overvejer mere bredt, hvordan data bevæger sig, og hvordan de er beskyttet, i din organisation. Alle organisationer skal træffe deres egne forholdsregler for at sikre overholdelse af reglerne med leverandørerne som vigtige partnere på denne færd.

Dataminimering

En vigtig del af GDPR's databeskyttelse som design ("Privacy By Design") er, at organisationer skal udvikle deres tjenester på en måde, der minimerer data. Det betyder at have god gennemsigtighed og kontrol med data i din organisation for at hjælpe dig med at administrere dem. Dashboard for administratorer i Dropbox Business er et nyttigt værktøj til at hjælpe med dette, da det gør det muligt for dig at overvåge teamets aktiviteter, få vist tilsluttede enheder og kontrollere delingsaktiviteter. Vi arbejder på at integrere principperne for databeskyttelse som design ("Privacy By Design") i nye produkter og funktioner.

Beskyttelse og gendannelse af data

Beskyttelse af mistede enheder, versionshistorik og filgendannelse kan være med til at beskytte mod utilsigtet tab, beskadigelse eller ødelæggelse af persondata, og det kan hjælpe med hurtigt at gendanne tilgængeligheden af og adgangen til persondata, hvis der indtræffer en hændelse. To-faktorgodkendelse er et andet vigtigt middel til at beskytte dine data.

Opbevaring af fortegnelser

GDPR giver også organisationer større forpligtelser til at gemme detaljerede fortegnelser om deres behandlingsaktiviteter. Vores overvågningslogge og aktivitetslogge kan hjælpe dig med bedre at forstå dine behandlingsaktiviteter som støtte for din registrering

Administration af adgang

Fra dashboard for administratorer i Dropbox Business kan du nemt administrere teammedlemmernes adgang til filer, mapper og Paper-dokumenter. For links til delte filer giver vores funktion til linkadgang dig mulighed for at beskytte de delte links med adgangskoder, angive udløbsdatoer for at give midlertidig adgang og begrænse adgangen til personer i din organisation. Hvis brugernes ansvarsområder ændres, gør vores værktøj til kontooverførsel det nemt for dig at overføre filer og ejerskab til Paper-dokumenter fra én bruger til en anden.

Administratorer kan også deaktivere en brugers adgang til sin konto og samtidig gemme deres data og delingsrelationer for at beskytte organisationens oplysninger.

Og endelig kan du bruge funktionen til fjernsletning til at slette filer og Paper-dokumenter fra enheder, der er blevet væk eller stjålet.

EU-infrastruktur

Selvom GDPR ikke kræver, at persondata skal opbevares inden for EU, tilbyder Dropbox kvalificerede Dropbox Business- og Dropbox Education-kunder mulighed for at gemme filer (blokke) i EU. EU-baseret fillagring leveres på Amazon Web Services' (AWS) infrastruktur. Hvis du vil have yderligere oplysninger om vores EU-infrastruktur, er du velkommen til at [kontakte vores salgsteam](#).

Samarbejde for at beskytte dine personlige data

Dropbox samarbejder med sine brugere om at beskytte deres personlige data. Vi træffer omfattende foranstaltninger for at beskytte vores infrastruktur, netværk og applikationer, uddanner medarbejdere i sikkerhed og beskyttelse af personlige oplysninger, og vi skaber en kultur, hvor det at være værdige til tillid har højeste prioritet,

og sætter vores systemer og praksis gennem streng testning og revision fra tredjepart.

Imidlertid spiller brugerne også en nøglerolle i beskyttelsen af deres personlige data.

Med Dropbox kan du konfigurere, bruge og overvåge din konto på måder, der opfylder din organisations behov for beskyttelse af

persondata, sikkerhed og overholdelse. Vores [delte ansvarsvejledning](#) kan hjælpe dig med at forstå mere om, hvad vi gør for at holde din konto sikker, og hvad du kan gøre for at bevare synlighed og kontrol over dine personlige data.

Konklusion

Hver dag sætter millioner af brugere deres lid til Dropbox. For at vise os værdige til denne tillid har vi opbygget, og vil fortsat opbygge, Dropbox med vægt på sikkerhed og beskyttelse af personlige oplysninger. Vores engagement i at beskytte brugernes personlige data udgør kernen i alle de beslutninger, vi træffer. Du kan få yderligere oplysninger ved at sende e-mail til privacy@dropbox.com. Hvis du ønsker yderligere oplysninger om GDPR, kan du også besøge vores [GDPR- vejledningscenter](#).