

Beskyttelse af personlige oplysninger og data

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 vores ansvar for at beskytte dine personlige data alvorligt.

Vores forpligtelser over for dig

Vi prioriterer beskyttelsen af dine persondata. Dropbox' [persondatapolitik](#) beskriver, hvordan vi indsamler, anvender og håndterer persondata, når du benytter vores tjenester. Vi prioriterer også at dele information om vores praksis angående persondata på en måde, der er nem at forstå. Ud over dette dokument har vi også gjort [ofte stillede spørgsmål om persondatapolitikken](#) tilgængelige for at besvare hyppige spørgsmål.

Hvis du har bopæl i Nordamerika (USA, Canada og Mexico), fungerer Dropbox, Inc. som din tjenesteudbyder. For alle andre brugere fungerer Dropbox International Unlimited Company som "dataansvarlig" for dine persondata. En dataansvarlig bestemmer formål med og midler til behandling af persondata.

Hvis du bruger en af vores Dropbox til teams-planer (for eksempel Dropbox Business eller Dropbox Education), fungerer din organisation som den dataansvarlige for alle persondata, der leveres til Dropbox i forbindelse med din brug af Dropbox. I dette tilfælde fungerer Dropbox som databehandler, der behandler data på vegne af din organisation i overensstemmelse med vores [virksomhedsaftale](#), der beskriver vores forpligtelser i forbindelse med databehandling og internationale dataoverførsler.

Uanset din plan anvender Dropbox de samme principper, hvad angår håndtering af dine persondata.

De følgende afsnit beskriver vores virksomhedsprincipper og giver et indblik i, hvordan vi overholder globale certificeringer og persondatabestemmelser.



Principper for dataanmodninger fra myndighederne

Vi er klar over, at brugerne forventer, at vi holder deres persondata fortrolige, når de betror os med de data. Som de fleste andre onlinetjenester modtager Dropbox af og til anmodninger fra myndigheder og retsinstanter, der efterspørger oplysninger om vores brugere. Vi gennemgår nøje hver enkelt anmodning og bestræber os på at give brugerne besked i henhold til loven, når deres konti identificeres i en anmodning.

Vi laver løbende en gennemsigtighedsrapport og har etableret følgende sæt principper for henvendelser fra myndigheder:

Vær åbne

Onlinetjenester bør have ret til at offentliggøre, hvor mange og hvilke typer anmodninger de modtager fra myndigheder, og til at underrette de personer, myndighederne ønsker information om. Denne form for åbenhed styrker brugerne ved at give dem bedre viden om tilfælde og mønstre af 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.

Lever tjenester, man kan have tillid til

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

Beskyt alle brugere

Love, der giver mennesker forskellig beskyttelse, afhængigt af hvor de bor eller deres statsborgerskab, er forældede og afspejler ikke onlinetjenesters globale natur.

Disse principper samt vores årlige gennemsigtighedsrapport er tilgængelige på Dropbox' websted: [Dropbox' oversigt over gennemsigtighed](#).

Principper for kunstig intelligens

Nogle af Dropbox' funktioner leveres ved hjælp af kunstig intelligens (AI). Dropbox arbejder for at sikre, at vores AI-innovationer ikke kun tjener vores kunder, men også respekterer deres rettigheder og sikkerhed.

Følgende principper er retningslinjer for vores teams i vores udvikling af AI-produkter og -funktioner på ansvarlig vis:

- Bruge AI til at betjene vores kunder
- Sikre, at kunderne har kontrol over deres data
- Være gennemsigtige om, hvordan vi bruger AI
- Arbejde for fairness inden for AI-teknologi
- Være ansvarlige over for vores kunder
- Respekttere mennesker, deres sikkerhed og deres rettigheder

Disse principper beskrives mere detaljeret på Dropbox' websted: [Dropbox' AI-principper](#).



Dropbox-kontrol: Vores interne praksis

Vi træffer omfattende foranstaltninger for at beskytte vores infrastruktur, netværk og applikationer. Nogle af vores sikkerhedsforanstaltninger er kryptering i hvile, kryptering under transit og adgangskontroller. Disse foranstaltninger beskrives i detaljer i [Dropbox' hvidbog om sikkerhed](#).

Vores robuste sikkerhedskontrol komplementeres af en række kontrolforanstaltninger vedrørende persondata. Her er nogle eksempler:



Persondatatræning

En del af beskyttelsen af vores brugeres persondata består i at skabe og fremme en kultur med opmærksomhed på at beskytte persondata. Dropbox' medarbejdere skal acceptere en persondatapolitik vedrørende brugerdata samt politik for dataklassificering, før de får adgang til systemerne. Kun medarbejdere med et specifikt behov har adgang til sådanne systemer. Medarbejdere deltager også i obligatorisk træning i beskyttelse af persondata på årsbasis. I denne træning undervises i det grundlæggende i persondatalovgivning og beskrives bedste praksis for at håndtere persondata hos Dropbox.



Anonymisering og pseudonymisering

I visse tilfælde, hvor vi ikke længere har brug for, at data kan henføres til en person, anvender vi metoder som anonymisering og pseudonymisering til at afidentificere dataene. Ved anonymisering fjernes eller ændres persondata permanent, så de ikke kan bruges til at identificere en person. Ved pseudonymisering fjernes eller ændres persondata midlertidigt, men processen kan omgøres, hvis nogen har adgang til yderligere information. Et eksempel på vores brug af pseudonymisering er, når vi afidentificerer kundefeedback og bruger det til at forbedre vores produkter og tjenester.



Permanent sletning af filer og Paper-dokumenter

Når en Dropbox-bruger eller en administrator for en Dropbox til teams-konto markerer en fil til permanent sletning, udløser det en proces til permanent sletning af filen. Når en bruger eller en administrator af en Dropbox til teams-konto markerer et Paper-dokument til permanent sletning, er der på samme måde en lignende proces til permanent at slette Paper-dokumentdata og -billedata.



Forvaltning af persondata

Teamet for beskyttelse af persondata er ansvarligt for driften af Dropbox' persondataprogram. Det implementerer vores vigtigste initiativer for beskyttelse af persondata og fører an med databeskyttelse gennem design i vores datalivscyklus. Dropbox' persondataprogram understøttes yderligere af flere tværfunktionelle underteamer på tværs af den juridiske afdeling og sikkerhedsafdelingen. Disse underteamer giver den ekstra ekspertise, der kræves for at udføre og føre tilsyn med de daglige opgaver i persondataprogrammet.

Den databeskyttelsesansvarliges kontor opererer separat fra andre persondatateams og skal overholde og føre tilsyn med beskyttelse af persondata. Kontoret kan kontaktes på privacy@dropbox.com.

Vores resultater: Overholdelse

En effektiv måde at vurdere en tjeneste på er, om den overholder regler og standarder. Vi tilskynder til og tilbyder uafhængig verificering af, at vores sikkerheds- og databeskyttelsespraksis overholder de bredest anerkendte standarder og bestemmelser såsom **ISO 27001, ISO 27017, ISO 27018, ISO 27701, HIIPA/HITECH, SOC 1, SOC 2 og SOC3**.

Vi er stolte af at have været en af de første leverandører af cloudtjenester, der opnåede certificering med ISO 27018, den internationalt anerkendte standard for førende praksis inden for beskyttelse af personlige oplysninger og data. Uafhængige tredjepartsrevisorer tester vores kontrolforanstaltninger og fremsætter deres rapporter og vurderinger. Vi deler disse med dig, når det er muligt. Bemærk, at mens omfanget af vores certificeringer og revisionsrapporter typisk henviser til Dropbox til teams, gælder størstedelen af vores kontrolforanstaltninger for alle Dropbox-planer.

Derudover overholder Dropbox **EU Cloud Code of Conduct**. EU Cloud Code of Conduct er et frivilligt redskab, der giver leverandører af cloudtjenester såsom Dropbox mulighed for at vise, at de prioriterer at overholde GDPR. Dropbox til teams er blevet erklæret i overensstemmelse med EU Cloud Code of Conduct og har modtaget et Compliance Mark på "niveau 2", som betyder, at disse tjenester har implementeret tekniske, organisatoriske og kontraktmæssige foranstaltninger i overensstemmelse med kravene i EU Cloud Code of Conduct. Du kan få mere at vide på det [officielle websted for EU Cloud Code of Conduct](#).

Du kan få mere at vide om de standarder, vi lever op til, og hvordan vi verificerer vores praksis, i vores [Trust Center](#) og på vores [webside om overholdelse af standarder og regler](#).

Internationale overførsler af data

Under overførsel af data fra Den Europæiske Union, Det Europæiske Økonomiske Samarbejdsområde, Storbritannien og Schweiz benytter Dropbox en række forskellige juridiske midler såsom kontrakter med vores kunder og associerede selskaber, standardkontraktbestemmelser og Europa-Kommissionens afgørelser om et tilstrækkeligt beskyttelsesniveau.

Dropbox overholder EU og USA's samt Schweiz og USA's rammer for databeskyttelse og den britiske udvidelse af EU og USA's rammer for databeskyttelse som fastsat af det amerikanske handelsministerium vedrørende behandling af persondata, der overføres fra EU, det Europæiske Økonomiske Samarbejdsområde, Storbritannien og Schweiz til USA. Dropbox har certificeret over for USA's handelsministerium, at det overholder disse rammer for databeskyttelse med hensyn til sådanne data, men dette omfatter ikke FormSwift-delen af tjenesterne.

Hvis du vil vide mere om rammen for databeskyttelse og se Dropbox' certificering, kan du besøge <https://www.dataprivacyframework.gov/>.

Klager og tvister i relation til vores overholdelse af rammen for databeskyttelse undersøges og løses gennem JAMS, en uafhængig tredjepart. Du kan få mere at vide i vores [persondatapolitik](#).

Andre, som arbejder for og med Dropbox

Dropbox administrerer selv størsteparten af aktiviteterne i forbindelse med levering af vores tjenester, men vi engagerer visse betroede tredjeparter i forbindelse med vores tjenester (for eksempel leverandører af kundesupport og IT-tjenester). Disse tredjeparter får kun adgang til dine oplysninger for at udføre opgaver på vores vegne i overensstemmelse med vores [persondatapolitik](#), og vi forbliver ansvarlige for deres håndtering af dine oplysninger i overensstemmelse med vores instruktioner.

Hver tredjepart gennemgår en streng kontrolproces, herunder sikkerhedsmæssige, databeskyttelsesmæssige og kontraktlige evalueringer for at vurdere 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 databeskyttelseslovgivning i forbindelse med behandling af persondata på Dropbox' vegne. Kunder kan følge Dropbox' betroede tredjeparter ved at gennemgå Dropbox' ISO 27001- og 27018-certificeringer. Under passende fortrolighedsforpligtelser kan kunderne også følge Dropbox' betroede tredjeparter ved at gennemgå Dropbox' kontrolforanstaltninger og revisionsresultater for Trust Services Criteria P6.1, P6.4 og CC.9.2 af SOC 2 Type II-rapporten.

Herudover kan Dropbox for at kunne levere tjenester til Dropbox til teams-kunder anvende underdatabehandlere med adgang til kunders persondata. Før vi anvender underdatabehandlere, udfører Dropbox due diligence angående underdatabehandlernes praksis for beskyttelse af persondata, sikkerhed og fortrolighed og træffer de nødvendige kontraktmæssige foranstaltninger med henblik på beskyttelse af persondata. Du kan se listen over underdatabehandlere og abonnere på ændringer i underdatabehandlinger ved at gå til vores [liste over underdatabehandlere](#).

Den generelle forordning om databeskyttelse

Den generelle forordning om databeskyttelse, også kaldet GDPR, er et EU-regulativ, der skaber et 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 betydeligt i overholdelse af GDPR.

Respekt for beskyttelse af persondata og sikkerhed har fra starten 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 på forkant 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 var overholdelse af GDPR en naturlig videreudvikling af vores eksisterende praksis og kontrolforanstaltninger.

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 databeskyttelsesekspertes bestående af juridiske rådgivere, specialister inden for sikkerhed og overholdelse samt produkt- og infrastrukturudviklere. Vores team udarbejdede derefter en komplet vurdering af vores praksis for sikkerhed og databeskyttelse i forhold til kravene i GDPR. Vores næste skridt var at evaluere vores aktiviteter forbundet med behandling af persondata og spore persondataenes livscyklus i vores systemer. Disse skridt kaldes undertiden udførelse af datakortlægning og gennemførelse af vurderinger af databeskyttelseseffekt.

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.

Du kan få mere information om GDPR i vores [GDPR-vejledningscenter](#).



Den registreredes rettigheder

GDPR giver enkeltpersoner ret til at tilgå, rette, slette og gøre indsigelse mod behandling af deres persondata. Disse forbrugerrettigheder kan også findes i en række andre databeskyttelseslove såsom California Consumer Privacy Act (CCPA). Sådan overholder Dropbox disse persondatarettigheder:



Ret til adgang og korrektion

Brugerne kan tilgå eller rette data om sig selv ved at logge på <https://www.dropbox.com> og gå til deres [kontoside](#). [Fanen "Generelt"](#) indeholder oplysninger såsom navnet og e-mailadressen forbundet med kontoen, [fanen "Sikkerhed"](#) viser IP-adresser på forbundne sessioner, computere og mobilenheder, og [fanen "Apps"](#) oplister de apps, der er forbundet med kontoen.

Dropbox har også lanceret [fanen "Persondata"](#), hvor brugerne kan generere adgangsrapporter. Enkeltpersoner, der ikke kan logge på deres konto, eller som ikke har en, kan indsende en anmodning om adgang til data ved at udfylde denne formular: [formular til anmodning om data](#).



Ret til sletning

Brugere, som ønsker at slette indhold på deres konto, kan gøre det direkte på deres konti. Du kan få mere at vide om at slette indhold [her](#).

Brugerne kan gå til fanen "Persondata" for at slette de af deres data, som ikke er relateret til deres konto (f.eks. kontaktoplysninger i vores marketingsystemer). Enkeltpersoner, der ikke kan logge på deres konto, eller som ikke har en, kan indsende en anmodning om sletning ved at udfylde denne formular: [formular til anmodning om data](#).



Ret til at gøre indsigelse

Afhængigt af behandlingsaktiviteten kan enkeltpersoner anmode om, at vi standser eller begrænser behandlingen af deres persondata. Hvis du ønsker at gøre indsigelse mod behandling af dine persondata, kan du sende os en e-mail på privacy@dropbox.com.

Enkeltpersoner kan til enhver tid fravælge at modtage marketingmateriale ved at ændre deres præferencer i sektionen [Meddelelser](#) på deres konto eller ved at klikke på afmeldingslinket i sidefoden i marketingmails.

Enkeltpersoner kan også fravælge indsamling af deres persondata ved hjælp af cookies ved at opdatere deres præferencer i Dropbox' cookiebanner. Du kan få mere at vide om Dropbox' brug af cookies og lignende teknologier på [denne side](#).

Styrkelse af vores brugere

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 gennem 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 til teams 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 gennem 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 overvågningslogs og aktivitetslogs kan hjælpe dig med bedre at forstå dine behandlingsaktiviteter som støtte for dine fortegnelser.



Administration af adgang

Fra dashboard for administratorer i Dropbox til teams kan du nemt administrere teammedlemmernes adgang til filer, mapper og Paper-dokumenter. For delte links til filer giver vores funktion til linktilladelser 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 vedkommendes data og delingsrelationer for at beskytte organisationens oplysninger. Endelig kan du bruge funktionen til fjernsletning til at slette filer og Paper-dokumenter fra bortkomne eller stjålne enheder.



EU-infrastruktur

Selvom GDPR ikke kræver, at persondata skal hostes inden for EU, tilbyder Dropbox kvalificerede Dropbox til teams-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 persondata

Dropbox samarbejder med sine brugere om at beskytte deres persondata. Vi har omfattende foranstaltninger for at beskytte vores infrastruktur, netværk og applikationer, vi uddanner vores medarbejdere i praksis inden for sikkerhed og beskyttelse af persondata, vi opbygger en kultur, hvor det har højeste prioritet at vise os værdige til tillid, og vi lader vores systemer og praksis gennemgå streng afprøvning og overvågning udført af tredjeparter.

Men brugerne spiller også en vigtig rolle i beskyttelsen af deres persondata. I Dropbox' [servicebetingelser](#) beskrives dit ansvar ved brug af vores tjenester. Med Dropbox kan du konfigurere, bruge og overvåge din konto på en måde, der lever op til din organisations behov for beskyttelse af persondata, sikkerhed og overholdelse af regler. Vores [vejledning til fælles ansvar](#) kan hjælpe dig til en bedre forståelse af, hvad vi gør for at beskytte din konto, og hvad du kan gøre for at bevare gennemsigtighed og kontrol i forbindelse med dine persondata.

Du kan få mere information om indholdet i dette dokument ved at sende en e-mail til privacy@dropbox.com.

