Dropbox

# Beskyttelse af personlige oplysninger og data

## Indledning

Personlige data spiller en meget stor rolle i samfundet og økonomien. Folk søger i stadig større grad kontrol med og indsigt i, hvordan deres personlige data anvendes og beskyttes af de organisationer, de har kontakt med. Samtidig ønsker folk, at organisationerne får klare retningslinjer for beskyttelse af personlige data.

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 forpligter os til at beskytte dine personlige data. Dropbox' Servicebetingelser beskriver dine forpligtelser, når du bruger vores tjenester. Vores Politik for 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 er bosiddende i Den Europæiske Union (EU), kontrolleres dine personlige data af Dropbox International Unlimited Company, som er baseret i Irland.

Hvis du bruger Dropbox Business eller Dropbox Education, fungerer din organisation som datakontrollør i forbindelse med eventuelle personlige data, der overdrages til Dropbox i forbindelse med din brug af Dropbox Business eller Dropbox Education. Datakontrolløren bestemmer formålet og midlerne i forbindelse med personlige data. Dropbox fungerer som databehandleren, som behandler data på vegne af din organisation, når du bruger Dropbox Business eller Dropbox Education, og vores Erhvervsaftale inkluderer vores forpligtelser i forbindelse med 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 f.eks. ISO 27001, ISO 27017, ISO 27018, den tyske BSI C5 og SOC 1, 2 og 3. For eksempel var vi 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 i cloud. Vores uafhængige tredjeparts revisorer tester vores kontrolforanstaltninger og leverer deres rapporter og meninger. Vi deler disse med dig, når det er muligt.

Bemærk, at selvom vores certificeringer og revisionsrapporter normalt refererer til Dropbox Business og Dropbox Education, gælder hovedparten af vores kontrolforanstaltninger også for brugere af Dropbox Basic, Plus og Professional. Du kan finde yderligere oplysninger om de standarder, vi overholder, og hvordan vi kontrollerer vores praksisser, på vores webside om overholdelse af regler.

Flere oplysninger om sikkerhedsfunktionerne og -politikkerne i Dropbox fås i hvidbogen om sikkerhed i Dropbox Business eller ved at kontakte sales@dropbox.com

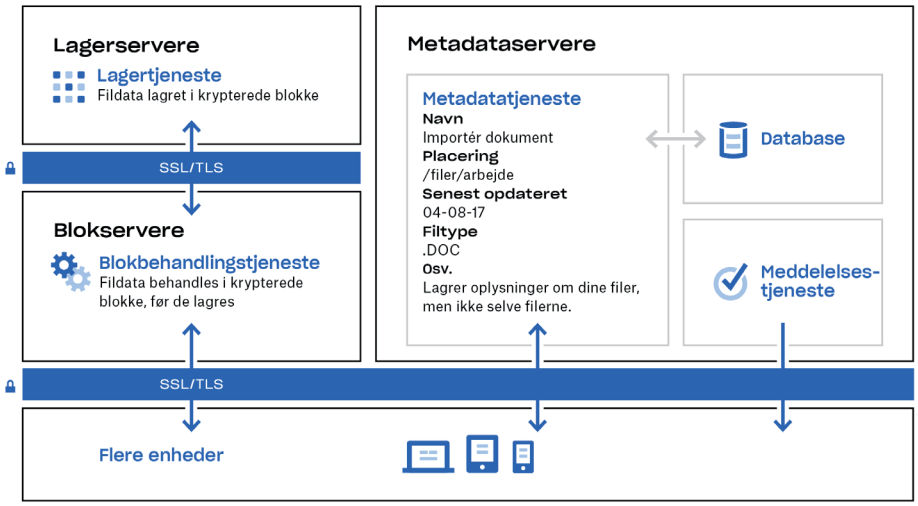
Dropbox

# 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: Filer

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




### Blokservere

Dropbox' design indebærer en unik sikkerhedsmekanisme, der består af mere end traditionel kryptering, til at beskytte brugerdata. 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 lagerserverne.

### Meddelelsestjeneste

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 meddelelsestjenesten og venter. Når der sker en ændring til en fil i Dropbox, giver meddelelsestjenesten besked om ændringen til den eller de pågældende klienter ved at lukke den lange forespørgselsforbindelse. Når forbindelsen lukkes, betyder det, at klienten skal oprette en sikker forbindelse til metadataserverne for at synkronisere eventuelle ændringer.

### Metadataservere

Visse grundlæggende oplysninger, der kaldes metadata, opbevares i deres egen særskilte lagertjeneste og fungerer som et indeks for dataene på brugernes konti. Dropbox-metadata opbevares i en MySQL-understøttet databasetjeneste og opdeles og kopieres efter behov for at opfylde kravene til ydeevne og høj tilgængelighed. 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.

### Lagerservere

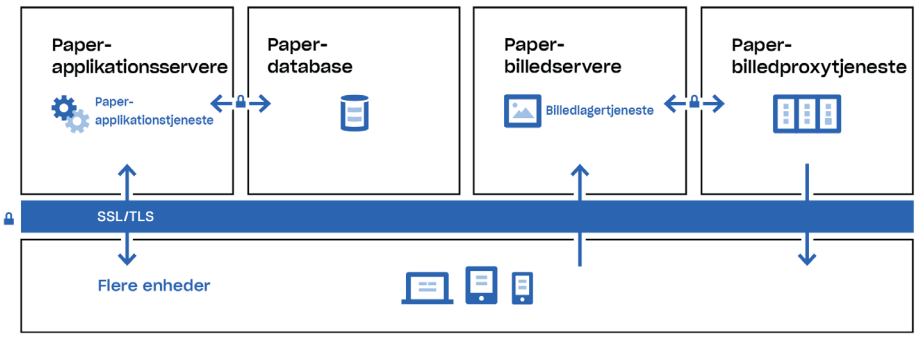
Når blokserverne har opdelt filerne i blokke og krypteret dem, bliver filernes faktiske indhold gemt på lagerserverne. Lagerserverne fungerer som et Content-Addressable Storage-system (CAS), hvor hver enkelt krypteret filblok hentes på baggrund af dens hash-værdi.

Flere oplysninger om sikkerhedsfunktionerne og -politikkerne i Dropbox fås i hvidbogen om sikkerhed i Dropbox Business eller ved at kontakte sales@dropbox.com

Dropbox

## 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 krypteres vha. en stærk krypteringsalgoritme.

### Paper-billedproxytjeneste

Paper-billedproxytjenesten viser billedeksempler for både billeder, som uploades til Paper-dokumenter, og til hyperlinks, som er integreret i Paper-dokumenter. For billeder, der uploades til Paper-dokumenter, henter Paper-billedproxytjenesten de billeddata, der er gemt på Paper-billedserverne, via en krypteret kanal. For hyperlinks, der er integreret i Paper-dokumenter, henter billedproxytjenesten billeddataene fra kildelinket og viser et eksempel på billedet vha. enten HTTP eller HTTPS, afhængigt af hvad der er specificeret i kildelinket.

### 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 mappetilknytninger 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-billedservere

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.

Dropbox

# Dropbox-kontrolelementer: Vores interne praksis

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. 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. Medarbejderne deltager også i obligatorisk uddannelse i sikkerhed og beskyttelse af personlige oplysninger for nye medarbejdere samt årlig opfølgende uddannelse. Medarbejderne modtager også regelmæssig opmærksomhedsuddannelse via oplysende e-mails, foredrag, præsentationer og ressourcer, som gøres tilgængelige på vores intranet.

## 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' lagerservere 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 Dropbox-bruger eller en administrator for et 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

Hvis brugerne ønsker andre oplysninger ud over de filer og Paper-dokumenter, der er gemt i Dropbox, kan de logge på webstedet og gå til deres kontosider. Kontosiden viser oplysninger som f.eks. det navn og den e-mailadresse, der er associeret med kontoen. Brugerne kan også få vist IP-adresser for tilsluttede sessioner, computere og mobilenheder samt apps, der er forbundet til deres konti, fra sikkerhedssiden og siden med tilsluttede apps.

Dropbox-brugere kan også anmode om adgang til eller sletning af andre personlige oplysninger, som vi kan have indsamlet om dem. Der er flere oplysninger om denne proces i Dropbox' Hjælpecenter.

Dropbox

### Principper for myndighedernes anmodninger 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.

#### Vær 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 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. 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 for at beskytte dine personlige data ved at besøge vores Hvidbog om sikkerhed i Dropbox Business.

## Andre, der arbejder for 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 Politik for beskyttelse af personlige oplysninger, og vi forbliver ansvarlige for deres håndtering af dine oplysninger i overensstemmelse med vores instruktioner. Hver tredjepart gennemgår en streng godkendelsesproces, herunder sikkerhedsgennemgange og regelmæssige kontraktbestemte revisioner, for at evaluere, om de er i stand til at overholde vores løfter om databeskyttelse.

## Internationale dataoverførsler

Dropbox forlader sig på en række juridiske mekanismer i forbindelse med sine internationale overførsler af personlige data fra EU til USA. Vi er certificeret i henhold til EU-U.S.- og Swiss-U.S. Privacy Shield-programmerne vedrørende indsamling, brug og opbevaring af personlige data og overførsel af disse fra EU og Schweiz til USA. Ud over Privacy Shield giver Dropbox også omfattende kontraktlige garantier vedrørende beskyttelse af personlige data i forbindelse med sine tjenester og forlader sig på EU's modelkontraktbetingelser til at dække sine internationale dataoverførsler.

Dropbox

# 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 gør forretninger i Europa, har investeret mange penge i overholdelse af GDPR.

Formålet med GDPR er at harmonisere databeskyttelseslovene i hele Europa og at opdatere dem, så de svarer til den hastige teknologiske udvikling, der er sket de seneste 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 med base i EU samt organisationer, der behandler EU-borgeres personlige data, skal overholde GDPR.

# Dropbox' bestræbelser for at overholde GDPR

Dropbox er fast besluttet på at overholde GDPR. Respekt for privatlivet 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 i konkurrencefeltet – 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 forretningsgange og kontrolforanstaltninger.

Dropbox' bestræbelser for at overholde GDPR begyndte, det øjeblik regulativet 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 skridt kaldes undertiden udførelse af datamappinger og gennemførelse af databeskyttelseseffektvurderinger.

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. Dette er vigtigt, eftersom GDPR sætter ekstra fokus på at dokumentere beslutninger og fremgangsmåder, der påvirker persondata.

Dropbox

# 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 det nye GDPR-krav om beskyttelse af personlige oplysninger som design ("Privacy By Design") er, at organisationer skal udvikle deres tjenester på en måde, der minimerer data. Det viat have god gennemsigtighed og kontrol med data i din organisation for at hjælpe dig med at administrere dem. Dropbox' dashboard for administratorer 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.

### 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 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 vores aktivitetslogge kan hjælpe dig med bedre at forstå dine behandlingsaktiviteter som støtte for din registrering.

### Administration af adgang

Fra Dropbox' dashboard for administratorer 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 i de fleste tilfælde 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.

Flere oplysninger om sikkerhedsfunktionerne og -politikkerne i Dropbox fås i hvidbogen om sikkerhed i Dropbox Business eller ved at kontakte sales@dropbox.com

Dropbox

# Samarbejde om at beskytte dine personlige data

Dropbox samarbejder med sine brugere om at beskytte deres personlige data. Vi har omfattende foranstaltninger for at beskytte vores infrastruktur, netværk og applikationer, vi uddanner vores medarbejdere i praksis inden for sikkerhed og beskyttelse af personlige oplysninger, 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 personlige data. Med Dropbox kan du konfigurere, bruge og overvåge din konto på en måde, der lever op til din organisations behov for beskyttelse af personlige oplysninger, sikkerhed og overholdelse af regler. Vores vejledning til delt 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 synlighed af og kontrol med 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 for 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.