

# Personvern og beskyttelse av data

Personopplysninger spiller en stor rolle i samfunnet og økonomien. Mennesker søker i økt grad bedre kontroll og klarhet om hvordan deres personopplysninger brukes og beskyttes av organisasjoner de samhandler med.

Hos Dropbox utgjør tillit grunnlaget for forholdet vårt med flere millioner mennesker og bedrifter over hele verden. Vi setter pris på tiltroen du gir oss og tar ansvaret for å beskytte informasjonen din på alvor.

## Våre forpliktelser til deg

Vi er forpliktet til å beskytte personopplysningene dine. Dropbox' [personvernerklæring](#) beskriver våre personvernforpliktelser og forklarer hvordan vi samler inn, bruker og håndterer dine personopplysninger når du bruker tjenestene våre. Vi er også forpliktet til å dele informasjon om vår personvernpraksis på en måte som er lett å forstå. Vi har gjort tilgjengelig en [Personvernerklæring: Ofte stilte spørsmål](#) samt dette dokumentet for å svare på vanlige spørsmål.

Hvis du bor i Nord-Amerika (USA, Canada og Mexico), vil Dropbox, Inc. fungere som din tjenestetilbyder. For alle andre brukere fungerer Dropbox International Unlimited Company som behandlingsansvarlig for dine personopplysninger. Den dataansvarlige bestemmer formål og midler for behandling av personopplysninger.

Hvis du bruker et av våre Dropbox for team-abonnementer (for eksempel Dropbox Business eller Dropbox Education), fungerer organisasjonen din som behandlingsansvarlig for alle personopplysninger som leveres til Dropbox i forbindelse med din bruk av Dropbox. I dette tilfellet fungerer Dropbox som databehandler, og behandler data på vegne av organisasjonen din i samsvar med vår [Forretningsavtale](#), som beskriver våre forpliktelser knyttet til databehandling og internasjonale dataoverføringer.

Uansett hvilket abonnement du har, bruker Dropbox de samme prinsippene når det gjelder håndtering av personopplysningene dine. I de følgende avsnittene beskriver vi selskapets prinsipper og gir et innblikk i hvordan vi overholder globale sertifiseringer og personvernforskrifter.



# Prinsipper for dataforespørsler fra myndighetene

Vi forstår at når brukerne betror oss personopplysningene sine, forventer de at vi holder dem konfidensielle. I likhet med andre netttjenester mottar Dropbox iblant forespørsler fra myndigheter og politimyndighetene som ønsker informasjon om brukerne våre. Vi går nøye gjennom alle dataforespørsler, og vi varsler brukerne når kontoene deres identifiseres i en forespørsel fra rettsinstanser, med mindre dette forbys ved lov.

Vi fører en åpenhetsrapport og har etablert følgende prinsipper for dataforespørsler fra myndighetene:

## Vis åpenhet

Netttjenester skal få lov til å publisere antall og typer statlige forespørsler de mottar, og å varsle folk når informasjon om dem har blitt etterspurt. Denne type åpenhet bemyndiggjør brukerne ved å hjelpe dem med å bedre forstå hendelser og mønstre av statlige inngrep. Vi vil fortsette å publisere detaljert informasjon om disse forespørslene og jobber for retten til å gi mer av denne viktige informasjonen.

## Bekjemp altfor brede forespørsler

Dataforespørsler av myndighetene bør være begrenset til informasjonen de søker og være snevert skreddersydd til bestemte personer og legitim etterforskning. Vi vil motstå generelle og altfor brede forespørsler.

## Levér tjenester brukerne kan stole på

Myndigheter burde aldri installere bakdører til netttjenester eller infiltrere infrastruktur for å innhente brukerdata. Vi kommer til å fortsette å jobbe for å beskytte systemene våre og endre lovene for å gjøre det klart at denne typen aktivitet er ulovlig.

## Beskytt alle brukere

Lover som gir personer ulik beskyttelse basert på hvor de bor eller statsborgerskap er foreldet og reflekterer ikke den globale karakteren til nettbaserte tjenester.

Disse prinsippene, sammen med vår årlige åpenhetsrapport, er gjort offentlig tilgjengelig på Dropbox-nettstedet på: [Oversikt over åpenhet i Dropbox](#).

# Prinsipper for kunstig intelligens

Noen av Dropbox' funksjoner er drevet av kunstig intelligens (AI). Dropbox arbeider for å sikre at våre AI-innovasjoner ikke bare tjener kundene våre, men også respekterer deres rettigheter og sikkerhet.

Følgende prinsipper veileder teamene våre når vi utvikler AI-produkter og -funksjoner på en ansvarlig måte:

- Utnyttelse av AI for å bedre betjene kundene
- Sørg for at kundene beholder kontrollen over dataene sine
- Være åpne om hvordan vi bruker AI
- Være en pådriver for rettferdighet innen AI-teknologi
- Stå til ansvar overfor våre kunder
- Respektere mennesker, deres sikkerhet og deres rettigheter

Disse prinsippene er beskrevet mer detaljert på Dropbox-nettstedet på: [Dropbox AI-prinsipper](#).



# Dropbox-kontroller: Vår interne praksis

Vi utfører omfattende tiltak for å beskytte infrastrukturen nettverket og applikasjonene våre. Noen av sikkerhetstiltakene vi har på plass inkluderer kryptering i ro, kryptering under transport og tilgangskontroll. Disse tiltakene er beskrevet i detalj i [Dropbox' hvitbok om sikkerhet](#).

Våre robuste sikkerhetskontroller suppleres av en rekke personvernkontroller. Noen eksempler er:



## Opplæring i personvern

En del av arbeidet med å beskytte brukernes personopplysninger handler om å bygge opp og utvikle en kultur for bevissthet rundt personvern. Dropbox-ansatte må godta en personvernerklæring for brukerdata og retningslinjer for dataklassifisering før de får tilgang til systemene. Bare de ansatte med et spesifikt behov har tilgang til slike systemer. Ansatte deltar også i obligatorisk opplæring i personvern på årlig basis. Disse kursene omfatter grunnleggende personvernlover og beskriver beste praksis for håndtering av personopplysninger hos Dropbox.



## Permanent sletting av filer og Paper-dokumenter

Når en Dropbox-bruker eller en administrator for en Dropbox for team-konto markerer en fil for permanent sletting, utløses det en prosess for permanent sletting av filen. På samme måte, når en bruker eller en administrator for en Dropbox for teams-konto markerer et Paper-dokument for permanent sletting, finnes det en lignende prosess for permanent sletting av Paper-dokumentdata og bildedata.



## Anonymisering og pseudonymisering

I visse tilfeller der vi ikke lenger har behov for at opplysningene skal kunne knyttes til en enkeltperson, bruker vi metoder som anonymisering og pseudonymisering for å aidentifisere opplysningene. Anonymisering fjerner eller endrer personopplysninger permanent slik at de ikke kan brukes til å identifisere en enkeltperson. Pseudonymisering fjerner eller endrer personopplysninger midlertidig, men prosessen kan reverseres hvis noen har tilgang til ytterligere informasjon. Et eksempel på når vi bruker pseudonymisering, er når vi aidentifiserer tilbakemeldinger fra kunder og bruker dem til å forbedre produktene og tjenestene våre.



## Forvaltning av personvern

Personvernteamet er ansvarlig for driften av Dropbox' personvernprogram. Det implementerer de viktigste personverninitiativene våre og er forkjemper for personvernet ved design i datalivssyklusen vår. Dropbox' personvernprogram støttes videre av flere tverrfunksjonelle underteam på tvers av de juridiske og sikkerhetsmessige avdelingene. Disse underteamene tilbyr den ekstra kompetansen som kreves for å drifte og føre tilsyn med de daglige oppgavene til personvernprogrammet.

Datatilsynets kontor opererer separat fra de andre personvernteamene, og har en funksjon for overholdelse av personvernregler og tilsyn. De kan kontaktes på [privacy@dropbox.com](mailto:privacy@dropbox.com).

## Vår merittliste: Etterlevelse

Samsvar er en effektiv måte å validere en tjenestes pålitelighet på. Vi oppfordrer til og er glade for å kunne tilby uavhengig bekreftelse på at vår sikkerhets- og personvernpraksis er i samsvar med de mest allment aksepterte standardene og forskriftene, for eksempel **ISO 27001, ISO 27017, ISO 27018, ISO 27701, HIPAA / HITECH, SOC 1, SOC 2, and SOC 3**.

Vi er stolte over å ha vært en av de første leverandørene av nettskytjenester som oppnådde sertifisering i henhold til ISO 27018, den internasjonalt anerkjente standarden for ledende praksis innen personvern og databeskyttelse i nettskyen. Vi har uavhengige, eksterne revisorer som tester kontrollene og avgir rapporter og tilbakemeldinger. Vi kan dele disse med deg når det er mulig. Vær oppmerksom på at selv om omfanget av sertifiseringene og revisjonsrapportene våre vanligvis refererer til Dropbox for team, gjelder de fleste av kontrollene våre for alle Dropbox-abonnementer.

I tillegg overholder Dropbox **EUs etiske retningslinjer for nettskyer**. EUs etiske retningslinjer for nettskyer er et frivillig instrument som gjør det mulig for en leverandør av nettskytjenester, som Dropbox, å demonstrere sin forpliktelse til å overholde GDPR. Dropbox for team har blitt erklært å være i samsvar med EUs etiske retningslinjer for nettskyer og har mottatt et samsvarsmerke på «nivå 2», noe som betyr at disse tjenestene har implementert tekniske, organisatoriske og kontraktsmessige tiltak i tråd med kravene i retningslinjene. For mer informasjon, besøk [retningslinjenes offisielle nettside](#).

Mer informasjon om standardene vi overholder og hvordan vi verifiserer praksisen vår, finner du i vårt [Trust Center](#) og på vår [nettside for samsvar](#).

## Internasjonale overføringer av data.

Når Dropbox overfører data fra EU, Det europeiske økonomiske samarbeidsområdet, Storbritannia og Sveits, er Dropbox avhengig av en rekke juridiske mekanismer, for eksempel kontrakter med våre kunder og tilknyttede selskaper, standard kontraktsklausuler og EU-kommisjonens beslutninger om tilstrekkelighet.

Dropbox handler i samsvar med personvernrammeverket mellom EU og USA og Sveits og USA, samt utvidelsen av personvernrammeverket mellom EU og USA for Storbritannia, som fastsatt av US Department of Commerce når det gjelder behandling av personopplysninger som overføres fra EU, EØS, Storbritannia og Sveits til USA. Dropbox har sertifisert til det amerikanske handelsdepartementet at de overholder disse rammeverkene for personvern med hensyn til slike data, men dette omfatter ikke FormSwift-delen av tjenestene.

For å finne ut mer om personvernrammeverket, og for å se Dropbox sin sertifisering, besøk [www.dataprivacyframework.gov](http://www.dataprivacyframework.gov).

Klager og tvister knyttet til etterlevelse av personvernrammeverket er etterforsket og løst gjennom JAMS, en uavhengig tredjepart. For å få vite mer, vennligst se vår [personvernerklæring](#).

## Andre som jobber for og med Dropbox

Dropbox håndterer de fleste aktivitetene når vi leverer tjenester, men bruker enkelte tiltrodde tredjeparter i den forbindelsen (for eksempel leverandører av kundestøtte og IT-tjenester). Disse tredjepartene får kun tilgang til opplysningene dine for å utføre oppgaver på vegne av Dropbox i samsvar med vår [personvernerklæring](#), og vi står ansvarlige for hvordan de håndterer opplysningene i samsvar med instruksene vi gir.

Alle tredjeparter gjennomgår en grundig vurderingsprosess, inkludert sikkerhets-, personvern- og kontraktsgjennomganger, for å evaluere deres evne til å oppfylle våre forpliktelser når det gjelder databeskyttelse. Basert på denne kritiske gjennomgangen stadfester Dropbox at de tiltrodde tredjepartene forplikter seg til å overholde EUs gjeldende personvernforordning i forbindelse med behandling av personopplysninger på Dropbox' vegne. Kunder kan overvåke Dropbox' betroede tredjeparter ved å gå gjennom Dropbox' ISO 27001- og 27018-sertifiseringer. Under passende konfidensialitetsforpliktelser kan kunder også overvåke Dropbox' betroede tredjeparter ved å undersøke Dropbox' kontroller og revisjonsresultater for tillitstjenestekriteriene P6.1, P6.4 og CC.9.2 i SOC 2 Type II-rapporten.

For å muliggjøre levering av tjenester for Dropbox for team-kunder, kan Dropbox i tillegg engasjere underdatabehandlere med tilgang til kundens personopplysninger. Før vi engasjerer underdatabehandlere, utfører Dropbox en grundig vurdering av underdatabehandlerens personvern-, sikkerhets- og konfidensialitetspraksis, og gjennomfører passende kontraktsmessige tiltak for beskyttelse av personopplysninger. Du kan se listen over underdatabehandlere og registrere deg for endringer av underdatabehandlere ved å gå til vår [liste over underdatabehandlere](#).

# Personvernforordningen

EUs personvernforordning (GDPR) er en EU-forordning som fastsetter et juridisk rammeverk for å beskytte personopplysningene til innbyggere i EU. Personvernforordningen er den viktigste europeiske loven om behandling av personopplysninger siden EUs personverndirektiv fra 1995, og mange selskaper – inkludert Dropbox – som har virksomhet i Europa har investert mye i etterlevelse av personvernforordningen.

Respekt for personvern og sikkerhet var en del av virksomheten vår helt fra starten av, og etter hvert som vi har vokst, har vi fortsatt å prioritere håndtering og beskyttelse av dataene som brukerne våre betror oss. Dropbox har gode resultater med å ligge i forkant av samsvarskurven – som beskrevet ovenfor var vi en av de første leverandørene av nettskytjenester som oppnådde ISO 27018-sertifisering for bedriftskundene våre. Med dette sterke fundamentet var GDPR-samsvar en naturlig videreutvikling av våre eksisterende rutiner og kontroller.

Dropbox' reise til etterlevelse av GDPR begynte så snart forordningen ble vedtatt i 2016. Vårt første skritt var å danne et tverrfunksjonelt team av spesialister for beskyttelse av data som består av juridiske rådgivere, fagfolk på sikkerhet og etterlevelse og produkt- og infrastruktureingeniører. Teamet vårt fullførte da en fullstendig vurdering av vår gjeldende praksis innen sikkerhet og beskyttelse av data, i lys av kravene til GDPR. Vårt neste steg var da å utføre en evaluering av aktivitetene våre ved behandling av personopplysninger og spore livssyklusen til personopplysninger gjennom systemene våre. Disse øvelsene blir noen ganger kalt påvirkningsevalueringer av utførelse av datakartlegging og fullføring av databeskyttelse.

Siden den gang har vi fortsatt å bygge på våre eksisterende interne prosesser og prosedyrer for å forsikre oss om at vi oppfyller prinsippene for ansvarlighet i henhold til kravene til GDPR, inkludert å føre register over behandling i samsvar med artikkel 30 i GDPR.

For mer informasjon om GDPR, besøk vårt [veiledningssenter for GDPR](#).



## Den registrertes rettigheter

Personvernforordningen gir enkeltpersoner rett til innsyn, retting, sletting og innsigelse mot behandlingen av personopplysningene deres. Disse forbrukerrettighetene finnes også i en rekke andre personvernlover, for eksempel California Consumer Privacy Act (CCPA). Slik overholder Dropbox disse personvernrettighetene:



### Rett til innsyn og korrigerings

Brukere kan få tilgang til eller korrigere data om seg selv ved å logge inn på <https://www.dropbox.com> og gå til [kontosiden](#). «[Generelt](#)»-fanen viser informasjon som navnet og e-postadressen som er knyttet til kontoen; «[Sikkerhet](#)»-fanen viser IP-adressene til tilkoblede økter, datamaskiner og mobile enheter, og «[Apper](#)»-fanen lister opp appene som er koblet til kontoen.

Dropbox har også lansert en «[Personvern](#)»-fane, der brukere kan generere tilgangsrapporter. Personer som ikke kan logge inn på kontoen sin, eller som ikke har en konto, kan sende inn en forespørsel om datatilgang ved å fylle ut dette skjemaet: [Forespørselsskjema for datasubjekt](#).



### Rett til sletting

Brukere som ønsker å slette innholdet på kontoen sin, kan gjøre det direkte fra kontoen sin. Mer informasjon om hvordan du sletter innhold [finner du her](#).

Brukere kan gå til «Personvern»-fanen for å slette data som ikke er relatert til kontoen (f.eks. kontaktinformasjon i markedsføringssystemene våre). Personer som ikke kan logge inn på kontoen sin, eller som ikke har en konto, kan sende inn en forespørsel om sletting ved å fylle ut dette skjemaet: [Forespørselsskjema for datasubjekt](#).



### Rett til innsigelse

Avhengig av behandlingsaktiviteten kan enkeltpersoner be om at vi stopper eller begrenser behandlingen av personopplysningene deres. Hvis du har innvendinger mot behandlingen av personopplysningene dine, kan du sende oss en e-post på [privacy@dropbox.com](mailto:privacy@dropbox.com).

Enkeltpersoner kan når som helst reservere seg mot å motta markedsføringsmateriell ved å endre preferansene sine i [Varslinger](#)-delen av kontoen sin, eller ved å klikke på koblingen Avslutt abonnement i bunnteksten i markedsførings-e-poster.

Enkeltpersoner kan også velge bort innsamling av personopplysninger gjennom informasjonskapsler ved å oppdatere preferansene sine i Dropbox-banneret for informasjonskapsler. For mer informasjon om Dropbox' bruk av informasjonskapsler og lignende teknologier, besøk [denne siden](#).

## Gi brukerne våre mer makt

Dropbox gir kontroll- og synlighetsfunksjoner som kan hjelpe deg å lettere administrere forpliktelsene dine for beskyttelse av data, inkludert GDPRs samsvarsforpliktelser. Samsvar med GDPR på tvers av organisasjonen din verken begynner eller slutter med forholdet ditt til leverandørene dine, som Dropbox. Selv om funksjonene våre hjelper deg å administrere forpliktelsene dine, kan de ikke alene sørge for samsvaret. Samsvar med GDPR krever at det tenkes bredere om hvordan data beveger seg rundt og er beskyttet i organisasjonen din. På reisen bør hver organisasjon ta sine egne skritt for å nå samsvar, både med leverandører og partnere.



### Dataminimering

Et viktig element i kravene til GDPRs innebygde personvern er at organisasjoner skal utforme tjenestene sine på en måte som innebærer dataminimering. Dette betyr å ha god synlighet og kontroll på dataene innad i organisasjonen for å hjelpe med å behandle den. Dropbox Business sitt administratorpanel er et nyttig verktøy for å hjelpe med dette, da det lar deg overvåke aktiviteten til et team, se tilkoblede enheter og revidere deling av aktivitet. Vi jobber for å integrere prinsippene for innebygget personvern i nye produkter og funksjoner.



### Beskyttelse og gjenoppretting av data

Beskyttelse av tapte enheter, versjonshistorikk og gjenoppretting av filer kan forebygge tap ved uhell, skader eller ødeleggelse av personopplysninger. Det kan bidra til å gjenopprette tilgjengelighet og tilgang til personopplysningene til rett tid i en situasjon der et uhell har skjedd. To-trinns-verifisering er et annet viktig mål vi anbefaler for å hjelpe med å beskytte dataen din.



### Arkivering

EUs personvernforordning øker også kravet om at organisasjoner må ha detaljerte arkiver om aktivitetene sine. Tilsynsloggene og aktivitetsloggene våre kan hjelpe deg med å forstå behandlingsaktivitetene dine bedre for å støtte registreringene dine.





### Administrering av tilgang

I administratorpanelet til Dropbox Business kan du enkelt administrere teammedlemmers tilgang til filer, mapper og Paper-dokumenter. For delte filkoblinger tillater koblingstillatelsesfunksjonen vår å beskytte delte koblinger med passord, sette utløpsdatoer for å gi midlertidig tilgang, samt begrense tilgang til disse i organisasjonen din. Dersom ansvaret skulle endres mellom brukere, lar verktøyet vårt for kontooverføring deg enkelt overføre filer og eierskap for Paper-dokumenter fra én bruker til en annen. Administratorer har også evnen til å deaktivere en brukers tilgang til deres konto samtidig som dataene og delingsforholdet blir bevart for å sikre informasjonen til organisasjonen din. Sist men ikke minst, funksjonen med ekstern sletting lar deg fjerne filer og Paper-dokumenter fra tapte eller stjålne enheter.



### EU-infrastruktur

Selv om GDPR ikke krever at personopplysninger skal lagres i EU, tilbyr Dropbox kvalifiserte Dropbox for teams-kunder muligheten til å lagre filer (blokker) i EU. EU-basert fillagring leveres på Amazon Web Services (AWS)-infrastruktur. Hvis du vil vite mer om EU-infrastrukturen vår, [kontakt salgsteamet vårt](#).

## Samarbeid for å beskytte personopplysningene dine

Dropbox samarbeider med brukerne sine for å beskytte deres personlige data. Vi iverksetter omfattende tiltak for å beskytte infrastrukturen vår, nettverket vårt og appene våre og vi lærer opp ansatte i sikkerhets- og personvernpraksis. Vi bygger en kultur hvor det å være verdig tillit er den høyeste prioritet og vi utsetter systemene og rutinene våre for grundig testing og revisjon via tredjeparter.

Brukerne spiller imidlertid også en nøkkelrolle når det gjelder å beskytte personopplysningene sine. Dropbox' [tjenestevilkår](#) beskriver ditt ansvar når du bruker tjenestene våre. Dropbox gjør det mulig for deg å konfigurere, bruke og overvåke kontoen din på måter som oppfyller organisasjonens behov for personvern, sikkerhet og samsvar. Vår [guide for felles ansvar](#) kan hjelpe deg med å forstå mer om hva vi gjør for å holde kontoen din trygg, og hva du kan gjøre for å opprettholde synlighet og kontroll over dine personlige data.

For mer informasjon om innholdet i dette dokumentet, send en e-post til [privacy@dropbox.com](mailto:privacy@dropbox.com).

