

Personvern og databeskyttelse

Introduksjon

Personopplysninger spiller en stor rolle i samfunnet og økonomien. I økende grad søker mennesker større kontroll og klarhet om hvordan personopplysningene deres brukes og beskyttes av organisasjoner de samhandler med.

Hos Dropbox er tillit grunnlaget for forholdet vi har til flere millioner mennesker og bedrifter over hele verden. Vi setter pris på tiltroen du gir oss, og tar ansvaret for å beskytte personopplysningene dine på alvor.

Våre forpliktelser til deg

Vi er opptatt av å beskytte personopplysningene dine. Dropbox' [vilkår for tjenester](#) skisserer ansvaret ditt når du bruker våre tjenester. Våre [personvernretningslinjer](#) beskriver våre personvernforpliktelser overfor brukere og forklarer hvordan vi samler inn, bruker og håndterer personopplysningene dine når du bruker tjenestene våre. Hvis du er bosatt i Nord-Amerika (USA, Canada og Mexico), opptreer Dropbox, Inc. som tjenesteleverandøren din.

For alle andre brukere, fungerer Dropbox International Unlimited Company som controller av personopplysningene dine.

Hvis du er bruker av Dropbox Business eller Dropbox Education, fungerer organisasjonen din som behandlingsansvarlig for all personlig informasjon som blir gitt til Dropbox i forbindelse med bruk av Dropbox Business eller Dropbox Education.

Behandlings ansvarlig bestemmer formålene og virkemidlene for behandling av personopplysninger. Dropbox fungerer som databehandler, behandler data på organisasjonens vegne når du bruker Dropbox Business eller Dropbox Education, og vår [Business-avtale](#) inkluderer forpliktelser relatert til databehandling og overføring av internasjonale data.

Vår merittliste: Etterlevelse

Etterlevelse er en effektiv måte å verifisere påliteligheten til en tjeneste på. Vi motiverer og er glade for å gi uavhengig bekreftelse på at vår sikkerhets- og personvernpraksis er i samsvar med de mest aksepterte standarder og forskrifter, for eksempel ISO 27001, ISO 27017, ISO 27018, HIPPA/HITECH, Tyskland BSI C5, og SOC 1, 2 og 3.

Videre var vi en av de første leverandørene av nettskytjenester til å oppnå sertifisering med ISO 27018, den internasjonalt anerkjente standarden for ledende fremgangsmåter innen personvern i nettskyen og databeskyttelse. Våre uavhengige tredjepartsrevisorer tester vår kontroll og gir oss rapportene og meningene deres. Vi kan dele disse med deg når det er mulig.

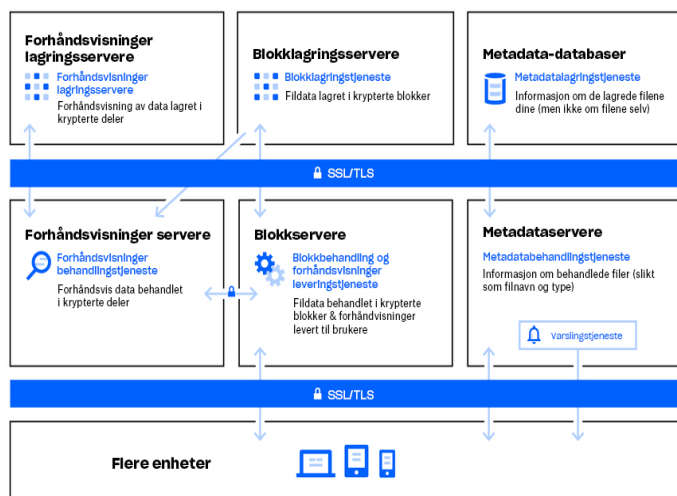
Vær oppmerksom på at mens omfanget av sertifiseringene og revisjonsrapportene vanligvis refererer til Dropbox Business og Dropbox Education, gjelder hoveddelen av kontrollene våre også for brukere av Dropbox Basic, Plus og Professional. Mer informasjon om standardene som vi overholder og hvordan vi verifiserer vår praksis, kan du finne på [websiden for overholdelse](#).

Dropbox Architecture: Beskytter dine personopplysninger

Hos Dropbox tror vi at beskyttelse av personopplysningene dine begynner med å holde dataene dine sikre. For det formålet er Dropbox designet med flere lag med beskyttelse, inkludert sikker filoverføring, kryptering og applikasjonsnivåkontroller som er fordelt over en skalerbar, sikker infrastruktur.

Infrastrukturen vår: Filer

Dropbox' infrastruktur for filer består av komponentene som er avbildet i diagrammet nedenfor.



Lagringsservere

Det faktiske innholdet i brukernes filer lagres i krypterte blokker med lagringsservere. Før overføring deler Dropbox-klienten filer i filblokker som forberedelse til lagring. Lagringsserverne fungerer som et CAS-system (Content-Addressable Storage), der hver enkelt krypterte filblokk hentes basert på hashverdien.

Forhåndsvisningsservere

Forhåndsvisningsserverne er ansvarlige for å produsere forhåndsvisninger av filer. Forhåndsvisninger er en gjengivelse av brukerens fil i et annet filformat som er mer egnet for rask visning på en sluttbrukers enhet. Forhåndsvisningsservere henter filblokker fra lagringsservere for å generere forhåndsvisninger. Når det blir bedt om en forhåndsvisning av fil, henter forhåndsvisningsserverne den hurtigbufrede forhåndsvisningen fra lagringsserverne for forhåndsvisning og overfører den til blokkserverne. Forhåndsvisninger vises til slutt til brukere av blokkservere.

Lagringsservere for forhåndsvisning

Bufrede forhåndsvisninger lagres i et kryptert format i lagringsserverne for forhåndsvisning.

Varslingstjeneste

Denne separate tjenesten er dedikert til å overvåke hvorvidt eventuelle endringer er utført for Dropbox-kontoer. Ingen filer eller metadata lagres eller overføres her. Hver klient etablerer en lang avspørringstilkobling til varslingstjenesten og venter. Når en hvilken som helst fil i Dropbox endres, signaliserer varslingstjenesten endringen til de(n) aktuelle kunden(e) ved å lukke den lange avspørringstilkoblingen. Lukking av tilkoblingssignalene signaliserer at klienten på en forsvarlig måte må koble til metadataserverne for å synkronisere eventuelle endringer.

Metadataservere

Enkelte grunnleggende opplysninger om brukerdataba, kalt metadata, oppbevares i sin egen diskrete lagringstjeneste og fungerer som en indeks for dataene i brukernes kontoer. Metadata inkluderer grunnleggende konto- og brukerinformasjon, som e-postadresse, navn og enhetsnavn. Metadata inkluderer også grunnleggende informasjon om filer, inkludert filnavn og typer, som hjelper deg med å støtte funksjoner som versjonshistorikk, gjenoppretting og synkronisering.

Metadata-databaser

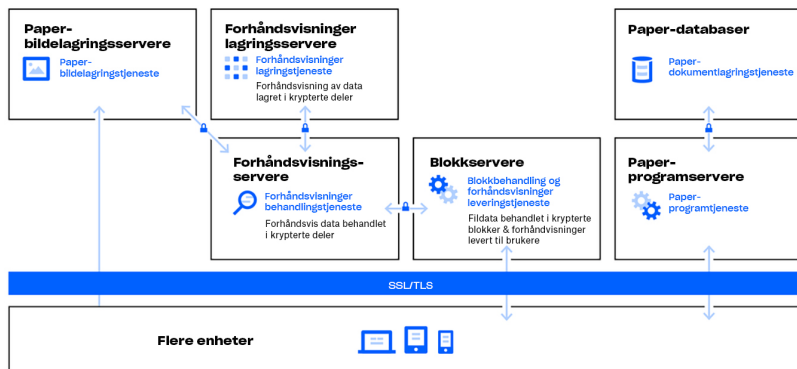
Filmetadata lagres i en MySQL-basert databasetjeneste, og er fragmentert og replikert etter behov for å oppfylle krav til ytelse og høy tilgjengelighet.

Blokk-servere

Ved design leverer Dropbox en unik sikkerhetsmekanisme som går utover tradisjonell kryptering for å beskytte brukerdataba. Blokkservere behandler filer fra Dropbox-applikasjonene ved å dele hver fil inn i blokker, kryptere hver blokk med en sterk chiffer og synkronisere bare de blokkene som er blitt endret mellom versjoner. Når en Dropbox-applikasjon oppdager en ny fil eller endringer i en eksisterende fil, varsler applikasjonen blokkserverne om endringen, og nye eller endrede filblokker behandles og overføres til lagringsserveren.

Vår infrastruktur: Paper

Dropbox Paper (Paper) er en funksjon i Dropbox-produktet. Imidlertid bruker Paper et stort sett forskjellige systemer i Dropbox-infrastrukturmiljøet. Papers infrastruktur består av komponentene som er avbildet i diagrammet under.



Paper-applikasjonsservere

Paper-applikasjonsservere behandler brukerforespørsler, gjengir resultatet av endrede Paper-dokumenter tilbake til brukeren, og utfører varslingstjenester. Paper-applikasjonsservere skriver inngående brukerendringer til Paper-databaser, der de plasseres for varig lagring. Kommunikasjonsøker mellom Paper-applikasjonsservere og Paper-databaser er kryptert med en sterk chiffer.

Paper-databaser

Det faktiske innholdet i brukernes Paper-dokumenter, i tillegg til visse metadata om disse Paper-dokumentene, krypteres for varig lagring i Paper-databasene. Dette omfatter informasjon om et Paper-dokument (for eksempel tittel, delte medlemskap og tillatelser, prosjekt- og mappetilknøyninger og annen informasjon), og selve innhold i Paper-dokumentet, inkludert kommentarer og oppgaver. Paper-databasene deles opp og replikeres etter behov for å oppfylle ytelseskrav og krav om høy tilgjengelighet.

Paper-bildeservere

Bilder som lastes opp til Paper-dokumenter, lagres og krypteres på Paper-bildeservere. Overføring av bildedata mellom Paper-applikasjonsservere og Paper-bildeservere foregår kryptert.

Forhåndsvisningsservere

Forhåndsvisningsserverne produserer forhåndsvisninger både for bilder som er lastet opp til Paper-dokumenter, samt hyperkoblinger som er innebygd i Paper-dokumenter. For bilder som er lastet opp til Paper-dokumenter, henter forhåndsvisningsserverne bildedata som er lagret i Paper-bildeservere via en kryptert kanal. For hyperkoblinger som er innebygd i Paper-dokumenter, henter forhåndsvisningsservere bildedataene og gjengir en forhåndsvisning av bildet ved hjelp av kryptering som spesifisert av kildekoblingen. Forhåndsvisninger vises til slutt til brukere av blokkservere.

Lagringsservere for forhåndsvisninger

Paper bruker de samme lagringsserverne for forhåndsvisninger som er beskrevet i Dropbox-infrastrukturdiagrammet for lagring av hurtigbufrede forhåndsvisninger av bilder. Hurtigbufrede forhåndsvisninger lagres i et kryptert format i lagringsserverne for forhåndsvisning.

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 permanent sletting av filer. Vi tilbyr også solid opplæring i personvern og sikkerhet for alle våre ansatte for å bygge en kultur der det å være tilliten verdig er en prioritet. Detaljer om noen av våre kontroller er beskrevet nedenfor:

Opplæring

En del av å beskytte våre brukeres personopplysninger innebærer å bygge og dyrke en kultur for sikkerhet og personvernbevissthet. Dropbox-medarbeidere er pålagt å godta retningslinjer for sikkerhet, inkludert personvernregler for brukerdata, før de får systemtilgang. Bare de ansatte med et spesifikt behov har tilgang til slike systemer. Ansatte deltar også på obligatorisk opplæring i sikkerhet og personvern på årlig basis.

Kryptering i transitt

For å beskytte fildata under transport mellom en Dropbox-klient (for øyeblikket skrivebord, mobil, API eller web) og Dropbox sine frontendservere, forhandles det om en kryptert tilkobling for å sikre sikker levering. Tilsvarende forhandles det om en kryptert forbindelse for å beskytte Paper-dokumentdata under transport mellom en Paper-klient (for tiden mobil, API eller web) og den vertsbaserte tjenesten. Disse tilkoblingene er kryptert ved hjelp av Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for å lage en sikker tunnel beskyttet av 128 bits Advanced Encryption Standard (AES)-kryptering eller høyere.

Kryptering i ro

Filer lastet opp av brukere lagres på Dropbox' lagringsservere som diskrete filblokker. Hver blokk er kryptert ved å bruke 256 bits Advanced Encryption Standard (AES). Kun blokker som

er endret mellom revisjoner, synkroniseres. Likedan, Paper-dokumentdata som lagres i Paper-databaser, krypteres i ro ved bruk av 256 bits Advanced Encryption Standard (AES).

Permanent sletting av filer og Paper-dokumenter

Når en Dropbox-bruker eller administrator for et Dropbox Business- eller Dropbox Education-team merker en fil for permanent sletting, utløser det en prosess for å slette filen permanent. På samme måte når en bruker, eller en administrator for et Dropbox Business- eller Dropbox Education-team merker et Paper-dokument for permanent sletting, er det en lignende prosess for å slette Paper-dokumentdata og billedata permanent.

Forespørsler om personopplysninger

For tilgang til personopplysninger utover filene og Paper-dokumentene som er lagret med Dropbox, kan brukere logge seg på nettstedet og gå til deres [konto sider](#). Kontosiden viser informasjon som navn og e-postadresse tilknyttet kontoen. Brukere kan også se IP-adressene til tilkoblede sesjoner, datamaskiner og mobile enheter, samt apper som er koblet til kontoene deres fra [sikkerhetssiden](#) og [tilknyttet appside](#).

Dropbox-brukere har også muligheten til å be om tilgang til eller sletting av andre personopplysninger som Dropbox kan ha samlet om dem. Mer informasjon om denne prosessen finner du i [Dropbox-hjelpesenter](#).

Personvernstyring hos Dropbox

Personvernprogramteamet er ansvarlig for å betjene Dropbox-personvernprogrammet. Det implementerer de viktigste personverninitiativene våre og er forkjemper for personvernet ved design i datalivssyklusen vår. Dropbox-personvernprogrammet støttes i tillegg av flere tverrfunksjonelle juridiske underteam. Disse underteamene tilbyr den ekstra kompetansen som kreves for å drifte og føre tilsyn med de daglige oppgavene til personvernprogrammet.

DPO-teamet opererer atskilt fra de andre personvernfunksjonene og er tjener til etterlevelse av personvern og tilsyn, og støtter personvernombudet direkte i utførelsen av oppgavene sine. Personvernombudet (DPO) er EUs lokale representant og kan kontaktes på privacy@dropbox.com.



Prinsipper for dataforespørslers fra myndighetene

Vi forstår at når brukere overlater personopplysningene sine til oss, forventer de at vi behandler disse dataene konfidensielt. Som de fleste tjenesteytere på nettet mottar Dropbox iblant forespørslers fra myndighetene som søker informasjon om brukerne.

Prinsippene nedenfor beskriver hvordan vi håndterer dataforespørslers vi mottar fra det offentlige.

Være åpen

Vi mener at onlinetjenester bør få lov til å publisere antall og typer forespørslers de mottar fra myndighetene, og å varsle enkeltpersoner når informasjon om dem har blitt etterspurt. Denne typen innsyn gir brukerne mulighet til å forstå in- stanser og mønstre når myndighetene går for langt. Vi vil fortsette å publisere detaljert

informasjon om disse forespørslene og går inn for retten til å utlevere mer av denne viktige informasjonen.

Bekjemp altfor brede forespørslers

Forespørslers om data fra myndighetene bør være begrenset i informasjonen de søker og snevert skreddersydd for bestemte personer og legitime undersøkelser. Vi vil motstå masseforespørslers og altfor bredt anlagte forespørslers.

Leverer tjenester brukerne kan stole på

Myndighetene må aldri installere bakdører til nettjenester 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 forskjellig beskyttelse basert på hvor de bor eller statsborgerskapet deres, er utdaterte og gjenspeiler ikke den globale karakteren til nettjenester. Vi vil fortsette å gå inn for en reform av disse lovene.

Disse prinsippene, sammen med vår årlige innsynsrapport, gjøres offentlig tilgjengelige på Dropbox-nettstedet på: <https://www.dropbox.com/transparency>.

For ytterligere informasjon om våre kontroller og vår tilnærming til å beskytte personopplysningene dine, vennligst se [Dropbox Business-hvitbok for sikkerhet](#).

Andre som jobber for og med Dropbox

Dropbox administrerer de fleste aktiviteter relatert til tilbudet av våre tjenester. Vi bruker imidlertid noen pålitelige tredjeparter i forhold til tjenestene våre (for eksempel leverandører av kundestøtte og IT-tjenester). Disse tredjepartene

får bare tilgang til informasjonen din for å utføre oppgaver på våre vegne i samsvar med våre [personvernretninglinjer](#), og vi vil fortsatt være ansvarlig for deres håndtering av informasjonen din i samsvar med instruksjonene våre.

Hver tredjepart gjennomgår en streng bakgrunnssjekk, inkludert sikkerhetsgjennomgang og regelmessige kontraktmessige gjennomganger, for å evaluere kvalifikasjonene deres til å oppfylle våre forpliktelser til databeskyttelse.

Internasjonale dataoverføringer

Dropbox er avhengig av en rekke juridiske mekanismer for internasjonal overføring av personopplysninger fra EU til USA. Vi er sertifisert i henhold til EU-USA og Sveits-USA Shield-programmer angående

innsamling, bruk og oppbevaring av personopplysninger og overføring fra EU og Sveits til USA. I tillegg til Privacy Shield, leverer Dropbox sterke kontraktmessige garantier rundt

personvernet for tjenestene sine og har implementert EU Model Contract Clauses for å dekke de internasjonale dataoverføringene sine.

GDPR: Personvernforordningen

Personvernforordningen eller GDPR er en forordning fra EU som legger til grunn et nytt rammeverk for vern av personopplysningene til EU-borgere. GDPR er den viktigste delen av europeisk lovgivning for beskyttelse av personopplysninger siden EUs personverndirektiv fra 1995, og mange selskaper - inkludert Dropbox - som driver virksomhet i Europa har investert mye i overholdelse av GDPR.

GDPR harmoniserer databeskyttelseslovgivning over hele Europa og bringer den i samsvar med den raske teknologiske endringen som har skjedd de siste to tiårene.

Det bygger på tidligere juridiske rammer i EU, inkludert EUs personverndirektiv, og introduserer nye forpliktelser og forpliktelser for organisasjoner som håndterer personopplysninger, samt nye rettigheter for enkeltpersoner med hensyn til deres personopplysninger.

personopplysninger. Organisasjoner som er etablert i EU, så vel som organisasjoner som behandler personopplysninger om EU-borgere, er pålagt å overholde GDPR.

Dropbox' reise til GDPR-samsvar

Dropbox er forpliktet til å oppfylle GDPR. Respekten for personvern og sikkerhet ble bygget inn i vår virksomhet fra begynnelsen, og etter hvert som vi har vokst, har vårt fokus på å håndtere og beskytte dataene som brukerne våre betror til oss, fortsatt å være en prioritet. Dropbox har en merittliste for å holde seg foran på kurven for etterlevelse - som beskrevet over, var vi en av de første leverandørene av nettskytjenester som oppnådde ISO 27018-sertifisering for våre forretningsbrukere. Gitt dette sterke grunnlaget, ser Dropbox GDPR-etterlevelse som en utvikling av vår eksisterende praksis og kontroller, og representerer en pågående utvikling av et sett med tiltak for å sikre at personopplysningene til brukerne våre alltid er beskyttet.

Dropbox' reise til overholdelse av GDPR begynte så snart forordningen ble vedtatt i 2016. Vårt første skritt var å danne et tverrfunksjonelt team av databeskyttelsespecialister bestående av juridisk rådgiver, og fagpersoner på overholdelse og sikkerhet og produkt- og infrastruktureingeniører. Teamet vårt fullførte deretter en fullstendig vurdering av gjeldende sikkerhets- og databeskyttelsespraksis mot GDPR-kravene.

Vårt neste trinn var å utføre en evaluering av våre behandlingsaktiviteter for personopplysninger og spore livssyklusen for personopplysninger gjennom systemene våre. Disse øvelsene er noen ganger referert til som utføring av kartlegginger av

personlig og sensitiv informasjon og vurdering av personvernkonsekvenser.

Styrke våre brukere på GDPR-reisene deres

Dropbox tilbyr kontroll- og synlighetsfunksjoner som kan hjelpe deg med lettere å administrere forpliktelsene dine til databeskyttelse, inkludert forpliktelsene til overholdelse av GDPR. Selvfølgelig starter eller slutter ikke GDPR-etterlevelse på tvers av organisasjonen med forholdet til leverandørene dine, som for eksempel Dropbox. Selv om funksjonene våre kan hjelpe deg med å administrere forpliktelsene dine, kan de ikke sikre overholdelse i seg selv. Overholdelse av GDPR krever å tenke bredt anlagt på hvordan data beveger seg omkring og beskyttes i organisasjonen din. Hver organisasjon bør ta sine egne skritt for å oppnå overholdelse, med leverandører som viktige partnere på denne reisen.

Dataminimering

Et viktig element i GDPRs krav til personvern ved design er at organisasjoner bør designe tjenestene sine på en dataminimerende måte. Dette betyr å ha god synlighet og kontroll over dataene i organisasjonen din for å hjelpe deg med å administrere den. Dropbox Business-administratorpanel er et nyttig verktøy for å hjelpe med dette, ettersom det lar deg overvåke teamaktivitet, se tilkoblede enheter og aktiviteter for revisjonsdeling. Vi jobber for å innarbeide prinsippene for personvern ved design i nye produkter og funksjoner.

Beskyttelse og gjenoppretting av data

Beskyttelse for mistet enhet, versjonshistorikk og gjenoppretting av filer kan bidra til å beskytte mot utilsiktet tap, skade eller ødeleggelse av personopplysninger, og kan hjelpe med muligheten til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger til rett tid i tilfelle av en ikke planlagt hendelse. Tofaktorautentisering er et annet viktig tiltak som vi oppfordrer til for å beskytte dataene dine.

Journalføring

GDPR øker også forpliktelsene for organisasjoner til å føre detaljerte nedtegnelser over behandlingsaktivitetene. Våre tilsynslogger og våre aktivitetslogger kan hjelpe deg med å bedre forstå behandlingsaktivitetene dine for å støtte din journalføring.

Tilgangsadministrasjon

I Dropbox Business-administratorpanelet administrerer du enkelt tilgang for teammedlemmer til filer, mapper og Paper-dokumenter. Funksjonen for koblingstillatelser gir deg muligheten til å passordbeskytte delte filkoblinger, angi utløpsdatoer for å gi midlertidig tilgang samt begrense tilgangen til disse innenfor organisasjonen. I tilfelle ansvaret endres mellom brukere, lar kontooverføringsverktøyet ditt enkelt overføre filer og eierskap til Paper-dokumenter fra en bruker til en annen.

Administratorer har også muligheten til å deaktivere en brukers tilgang til kontoen sin, mens de bevarer dataene sine og deler relasjoner for å holde organisasjonens informasjon trygg. Til slutt, funksjonen for ekstern sletting

lar deg fjerne filer og Paper-dokumenter fra mistede eller stjålne enheter.

EU-infrastruktur

Mens GDPR ikke krever at personopplysninger skal lagres i EU, tilbyr Dropbox kvalifiserte kunder fra Dropbox Business og Dropbox Education muligheten til å lagre filer (blokker) i EU. EU-basert fillagring tilbys på Amazon Web Services (AWS)-infrastruktur. For å lære mer om EU-infrastrukturen vår, [kontakt salgsteamet vårt](#).



Jobber sammen for å beskytte personopplysningene dine

Dropbox samarbeider med brukerne sine for å beskytte personopplysningene deres. Vi utfører omfattende tiltak for å beskytte infrastrukturen, nettverket og applikasjonene våre, lærer opp ansatte i sikkerhets- og personvernpraksis, utvikler en kultur der høyeste prioritet er å være tilliten

verdig, og utsetter våre systemer og praksis for streng tredjepartstesting og revisjon.

Imidlertid spiller brukere også en nøkkelrolle i å beskytte personopplysningene sine. Dropbox setter deg istand til å konfigurere, bruke og overvåke kontoen din på

måter som dekker organisasjonens personvern, sikkerhet og overholdelsesbehov. Vår [veiledningfor delt ansvar](#) kan hjelpe deg 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 personopplysningene dine.

Oppsummering

Hver dag setter millioner av brukere sin tillit til Dropbox. For å være tilliten verdig utviklet vi og vil fortsette å utvikle Dropbox med vekt på sikkerhet og personvern. Vår forpliktelse til å beskytte brukernes personopplysninger er kjernen i hver beslutning vi tar. For mer informasjon, send e-post til privacy@dropbox.com. For mer informasjon om GDPR, kan du også besøke vårt [GDPR-veiledningssenter](#).