Dropbox

Personvern og beskyttelse av data

Innledning

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 tilliten du viser oss og tar ansvaret for å beskytte personopplysningene dine på alvor.

Våre forpliktelser overfor deg

Vi forplikter oss til å beskytte personopplysningene dine. Dropbox' tjenestevilkår oppsummerer hva du forplikter deg til når du bruker tjenestene våre. Personvernerklæringen beskriver hvilke forpliktelser vi har knyttet til brukernes personvern og forklarer hvordan vi samler inn, bruker og håndterer personopplysningene dine når du bruker tjenestene våre. Hvis du bor i Nord-Amerika (USA, Canada og Mexico), fungerer Dropbox Inc. som tjenesteleverandør. For alle andre brukere er det Dropbox International med ubegrenset ansvar opptrer som ansvarlig for personopplysningene dine.

Hvis du er Dropbox Business- eller Dropbox Education-bruker, fungerer organisasjonen din som behandlingsansvarlig for alle personopplysninger som er gitt til Dropbox i forbindelse med bruken din av Dropbox Business eller Dropbox Education. Den dataansvarlige bestemmer formål og midler for behandling av personopplysninger.

Dropbox fungerer som databehandler og behandler data på organisasjonens vegne når du bruker Dropbox Business eller Dropbox Education, og Business-avtalen vår inkluderer forpliktelser knyttet til databehandling og internasjonal dataoverføring.

Oppnådde resultater: Samsvar

Samsvar er effektivt for å vurdere hvor pålitelig en tjeneste er. Vi oppmuntrer til og tilbyr uavhengig kontroll av at sikkerhets- og personvernpraksisen vår er i samsvar med de mest anerkjente standardene og forskriftene, som ISO 27001, ISO 27017, ISO 27018, ISO 27701, HIPPA/HITECH og SOC 1, 2 og 3.

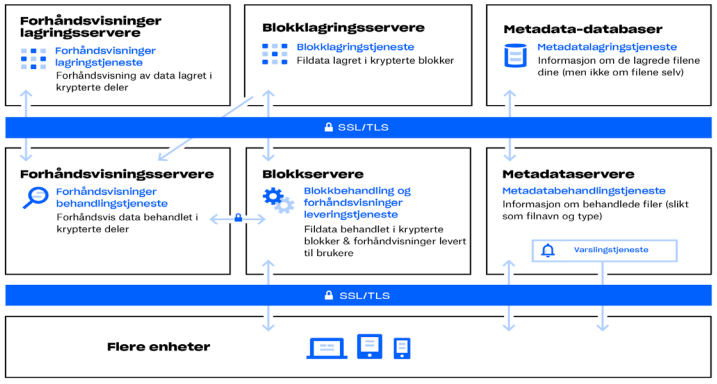
Vi var også en av de første leverandørene av nettskytjenester som ble ISO 27018-sertifisert. Dette er den internasjonalt anerkjente standarden for ledende praksis innen personvern for nettskyen og behandling av personopplysninger. Vi har uavhengige, eksterne revisorer som tester kontrollene og avgir rapporter og tilbakemeldinger. Vi kan dele disse med deg når det er mulig. Merk at selv om rammen av sertifiseringene og revisjonsrapportene våre typisk viser til Dropbox Business og Dropbox Education, så gjelder de fleste av kontrollene våre for brukere av Dropbox Basic, Plus og Professional også. I tillegg følger nå Dropbox EUs etiske retningslinjer for nettskyen. Mer informasjon om standardene vi etterlever og hvordan vi kontrollerer praksisene våre finner du på samsvarsnettsiden.

Dropbox-arkitektur: Beskyttelse av dine personopplysninger

Her på Dropbox mener vi at å beskytte din personlige data begynner med å holde dataen din sikker. Dropbox er utformet med flere lag av beskyttelse, inkludert sikker dataoverføring, kryptering og nivåkontroller for applikasjonen som er fordelt på en skalerbar, sikker infrastruktur.

Vår infrastruktur: Filer

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



Metadataservere

Visse typer grunnleggende informasjon om brukerdata, kalt metadata, lagres i sin egen atskilte lagringstjeneste og fungerer som en indeks for dataene på 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 å støtte funksjoner som versjonshistorikk, gjenoppretting og synkronisering.

Metadata-databaser

Filmetadata lagres i en MySQL-basert databasetjeneste, og deles og replikeres når nødvendig for å innfri høye krav til ytelse og tilgjengelighet.

Blokkservere

I utgangspunktet leverer Dropbox en unik sikkerhetsmekanisme som går utover tradisjonell kryptering for å beskytte brukerdata. Blokkservere behandler filer fra Dropbox-applikasjonene ved å dele opp hver fil i blokker, kryptere hver filblokk ved hjelp av en sterk kryptering og synkronisere bare blokker som er endret mellom revisjoner. Når en Dropbox-applikasjon oppdager en ny fil eller endringer på en eksisterende fil, varsler applikasjonen blokkserverne om endringen, og nye eller endrede filblokker behandles og overføres til lagringsserverne.

Blokklagringsservere

Det faktiske innholdet i brukernes filer lagres i krypterte blokker hos blokklagringsserverne. Før overføring deler Dropbox-klienten filene inn i filblokker for å forberede lagringen. Lagringsserverne fungerer som et Content-Addressable Storage-system (CAS), der hver enkelt krypterte filblokk hentes basert på hash-verdien dens.

Forhåndsvisningsservere

Forhåndsvisningsservere er ansvarlige for å opprette forhåndsvisning av filer. Forhåndsvisninger er en gjengivelse av en brukers fil i et annet filformat som er mer egnet for rask visning på en sluttbrukers enhet. Forhåndsvisningsservere gjenfinner filblokker fra lagringsservere å generere forhåndsvisning. Når det bes om forhåndsvisning av en fil, henter forhåndsvisningsservere den hurtigbufrede forhåndsvisningen fra lagringsservere for forhåndsvisning og overfører den til blokkservere. Forhåndsvisning leveres i siste instans av blokkservere til brukere

Lagringsservere for forhåndsvisning

Hurtigbufrede forhåndsvisninger lagres i et kryptert format på lagringsservere for forhåndsvisning.

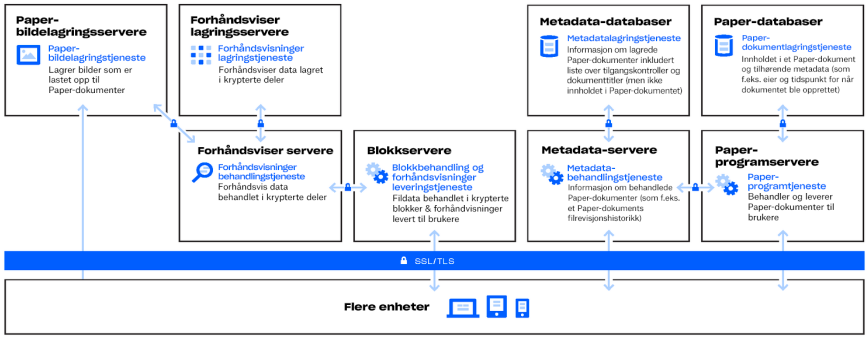
Meldingstjeneste

Denne separate tjenesten er viet til å overvåke hvorvidt eventuelle endringer er utført for Dropbox-kontoer. Ingen filer eller metadata lagres eller overføres her. Hver klient etablerer en «long poll»-tilkobling til varslingstjenesten og venter. Når en endring av en fil i Dropbox finner sted, signaliserer varslingstjenesten en endring til den eller de relevante klienten(e) ved å lukke «long poll»-tilkoblingen. Ved lukking av tilkoblingen signaliseres det at klienten på forsvarlig vis må koble til metadataserverne for å synkronisere endringer.

Dropbox

Vår infrastruktur: Paper

Dropbox Paper (Paper) er en funksjon i Dropbox-produktet. Imidlertid bruker Paper for det meste et distinkt sett med systemer i Dropbox-infrastrukturmiljøet. Paper sin infrastruktur består av komponentene i diagrammet nedenfor.



Programservere for Paper

Programservere for Paper behandler brukerforespørsler, gjengir produksjon av redigerte Paper-dokumenter tilbake til brukeren og utfører varslingstjenester. Programservere for Paper skriver innkommende brukerredigeringer til Paper-databasene, der de blir plassert i vedvarende lagring. Kommunikasjonsøkter mellom programservere for Paper og Paper-databaser er kryptert med en avansert kodenøkkel.

Paper-databaser

Det faktiske innholdet til brukernes Paper-dokumenter, så vel som visse metadata om disse Paper-dokumentene, er kryptert i vedvarende lagring i Paper-databasene. Dette inkluderer informasjon om et Paper-dokument (som for eksempel tittelen, delt medlemskap og tillatelser, prosjekt- og mappeassosiasjoner og annen informasjon), samt innhold i selve Paper-dokumentet, inkludert kommentarer og oppgaver. Paper-databasene fragmenteres og replikeres etter behov for å møte høye krav om ytelse og tilgjengelighet.

Bildeservere for Paper

Bilder som lastes opp til Paper-dokumenter er lagret og kryptert ved stillstand i bildeserverne til Paper. Overføring av bildedata mellom Paper-programmet og bildeserverne til Paper gjennomføres over en kryptert økt.

Forhåndsvisningsservere

Forhåndsvisningsservere leverer bildeforhåndsvisninger både for bilder som er lastet opp i Paper-dokumenter og for hyperkoblinger som er innebygd i Paper-dokumenter. For bilder som er lastet opp til Paper-dokumenter, vil forhåndsvisningsservere hente bildedata lagret i bildelagringsserverne til Paper gjennom en kryptert kanal. For hyperkoblinger som er innebygd i Paper-dokumenter, vil forhåndsvisningservere hente bildedata og gjengi en forhåndsvisning av bildet ved hjelp av kryptering som er angitt av kildekoblingen. Forhåndsvisning leveres i siste instans av blokkservere til brukere

Forhåndsvisningslagringsservere

Paper bruker de samme serverne for forhåndsvisningslagring som er beskrevet i diagrammet for Dropbox-infrastruktur for å lagre hurtigbufret forhåndsvisning av bilde. Hurtigbufrede deler av forhåndsvisning lagres i et kryptert format på forhåndsvisningservere.

Dropbox-kontroller: Vår interne praksis

Vi iverksetter omfattende tiltak for å beskytte infrastrukturen vår, nettverket vårt 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 robust opplæring i personvern og sikkerhet for alle ansatte for å utvikle en kultur der det å være tillit verdig er prioritert. Detaljer om noen av kontrollene våre er beskrevet nedenfor:

Opplæring

En del av det å beskytte brukernes personopplysninger innebærer å utvikle og bygge en kultur med fokus på sikkerhet og personvern. Dropbox-ansatte er pålagt å godta retningslinjene for sikkerhet, inkludert retningslinjer for personvern av brukerdata, 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 sikkerhet og personvern på årlig basis.

Kryptering under overføring

For å beskytte fildata under transport mellom en Dropbox-klient (for øyeblikket skrivebord, mobil, API eller web) og Dropbox' frontservere, forhandles det om en kryptert tilkobling for å sikre sikker levering. På samme vis er en kryptert forbindelse satt opp for å beskytte overførselen av Paper-dokumentdata mellom en Paper-klient (for tiden mobil, API eller nett) og vertstjenesten. Disse tilkoblingene krypteres ved hjelp av Secure Sockets Layer (SSL) / Transport Layer Security (TLS) for å lage en sikker tunnel beskyttet av 128-bits eller høyere Advanced Encryption Standard-kryptering (AES).

Kryptert lagring

Filer lastet opp av brukere er lagret på Dropbox sine lagringsservere som diskrete filblokker. Hver blokk er kryptert ved hjelp av en 256-bit Advanced Encryption Standard (AES).

Bare blokker som har blitt endret mellom revisjoner, blir synkronisert. På samme vis er Paper-dokumentdata lagret kryptert ved hjelp av en 256-bit Advanced Encryption Standard (AES) på Paper-databaser.

Slette filer og Paper-dokumenter permanent

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 bildedata permanent.

Personopplysninger og tilgangsforespørsler

For tilgang til personopplysninger utover filene og Paper-dokumentene som er lagret i Dropbox, kan brukere logge på nettstedet og gå til kontosidene deres. Kontosiden viser informasjon som navnet og e-postadressen som er knyttet til kontoen. Brukere kan også se IP-adressene til tilkoblede økter, datamaskiner og mobile enheter; samt apper som er koblet til kontoene sine fra sikkerhets siden og tilkoblede apper.

Dropbox-brukere har også mulighet til å be om tilgang til eller sletting av andre personopplysninger som Dropbox kan ha hentet inn. Mer informasjon om denne prosessen finner du i Dropbox hjelpesenter.

Personvernstyring hos Dropbox

Personvern teamet er ansvarlig for drift av Dropbox Privacy Program. Det implementerer våre viktigste personverninitiativer og støtter personvern innebygget i datalivssyklusen vår. Dropbox Privacy Program støttes videre av flere tverrfunksjonelle juridiske undergrupper. Disse undergruppene gir den tilleggskompetansen som kreves for å drive og overvåke de daglige oppgavene til personvernprogrammet.

DPO-teamet fungerer atskilt fra de andre personvernfunksjonene og fungerer som etterlevelse av personvern og tilsyn som direkte støtter databeskyttelsesansvarlig i utførelsen av pliktene deres. Datavernombudet (DPO) kan kontaktes på privacy@dropbox.com.

Dropbox

Offentlige data

Prinsipper for forespørsler

Vi forstår at når brukere betror seg til oss med deres personopplysninger, så forventes det av oss at vi holder dataen konfidensielle. Som de fleste nettbaserte tjenester, mottar Dropbox noen ganger forespørsler fra regjeringer som søker informasjon om brukerne.

Prinsippene nedenfor beskriver hvordan vi håndterer forespørsler om data fra myndighetene.

Vis åpenhet

Vi tror på at nettbaserte tjenester skal tillates å publisere antall og typer forespørsler fra myndighetene som de mottar og varsle enkeltpersoner når det er bedt om informasjon om dem. Denne typen transparens gir brukere mulighet til å hjelpe dem med å forstå forekomster og mønstre for myndighetenes iherdighet. 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 fra myndighetene bør være begrenset til informasjonen de søker og skreddersydd for spesifikke personer og legitime etterforskninger. Vi vil motstå generelle og altfor bredt anlagte forespørsler.

Lever pålitelige tjenester

Myndighetene bør aldri installere bakdører i elektroniske tjenester online eller kompromittere infrastruktur for å skaffe brukerdata. Vi vil fortsette å arbeide for å beskytte systemene våre og endre lover 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. Vi vil fortsette å jobbe for reform av disse lovene.

Disse prinsippene, sammen med vår årlige transparensrapport, er gjort offentlig tilgjengelig på Dropbox-nettstedet på: https://www.dropbox.com/transparency.

For mer informasjon om kontroller og tilnærming til beskyttelse av personopplysninger, se rapporten Dropbox Business Security.

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 våre retningslinjer for personvern, og vi står ansvarlige for hvordan de håndterer opplysningene i samsvar med instruksene vi gir.

Hver tredjepart underlegges en kritisk gjennomgang, inkludert gjennomganger av sikkerhet og personvern og regelmessige, kontraktsmessige gjennomganger, for å vurdere evnen til å overholde forpliktelsene våre når det gjelder behandling av personopplysninger. 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 få oversikt over Dropbox sine tiltrodde tredjeparter ved å se gjennom ISO 27001- og 27018-sertifiseringene til Dropbox, og, i samsvar med gjeldende krav til konfidensialitet, se gjennom SOC 2 Type II-rapporten. Kunder kan særlig få oversikt over Dropbox sine tiltrodde tredjeparter ved å se nærmere på kontroller og revisjonsresultater for tillitstjenestekriteriene P6.1, P6.4 og CC .9.2 i SOC 2 Type II-rapporten.

Dropbox

Internasjonale dataoverføringer

Ved overføring av data fra EU, EØS, Storbritannia og Sveits, er Dropbox avhengig av en rekke juridiske mekanismer, for eksempel kontrakter med våre kunder og tilknyttede selskaper, standard kontraktklausuler og EU-kommisjonens beslutninger om tilstrekkelighet om visse land, som aktuelt.

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 bekreftet til Department of Commerce at selskapet overholder personvernrammeverkene med hensyn til slike data, men det omfatter ikke DocSend- eller Formswift-delene av tjenestene.

For å finne ut mer om personvernrammeverket, og for å se Dropbox sin sertifisering, besøk 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.

GDPR: EUs personvernforordning

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. Personvernforordningen harmoniserer lover for behandling av personopplysninger i hele Europa og oppdaterer dem med hensyn til de raske teknologiske endringene som har funnet sted de siste to tiårene. Den bygger på tidligere juridiske rammeverk i EU, inkludert personverndirektivet, og introduserer nye forpliktelser og ansvar for organisasjoner som håndterer personopplysninger, i tillegg til nye rettigheter for enkeltpersoner når det gjelder personopplysninger. Organisasjoner som er etablert i EU, samt organisasjoner som behandler personopplysninger om innbyggere i EU, er forpliktet til å etterleve personvernforordningen.

Dropbox sin GDPR-samsvarsreise

Dropbox er forpliktet til å etterleve GDPR. Respekt for personvern og sikkerhet har vært innebygd i bedriften fra starten av, og med veksten vår, har fokuset vårt på håndtering og beskyttelse av data, som brukerne tillitsfullt har betrodd oss, vært en prioritet. Oppnådde resultater viser at Dropbox ligger i forkant på etterlevelseskurven. Som beskrevet ovenfor, var vi en av de første nettskytjenestene som oppnådde ISO 27018-sertifisering for bedriftskundene våre. Gitt dette sterke grunnlaget, ser Dropbox etterlevelse av GDPR som en utvikling av vår eksisterende praksis og kontroller, og representerer et kontinuerlig sett med tiltak som utvikler seg for å sikre at brukernes personopplysninger alltid er beskyttet. 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 infrastrukturingeniører. 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 fullførelse 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. Dette er viktig fordi GDPR legger et økt fokus på å dokumentere beslutninger og praksis som påvirker personopplysninger.

Styrking av brukerne våre på deres GDPR-reiser

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 dataminimalisering. Dette betyr å ha god synlighet og kontroll på dataen 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. Totrinnsgodkjenning er et annet viktig mål vi anbefaler for å hjelpe med å beskytte dataen dine.

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 koblingtillatelsesfunksjonen 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 rettigheter for Paper-dokumenter fra én bruker til en annen.

Administratorer har også muligheten til å deaktivere en brukers tilgang til kontoen sin, samtidig som dataene og delingsforholdet bevares 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 EUs personvernforordning ikke krever at personopplysninger skal være lagret i EU, tilbyr Dropbox kvalifiserte Dropbox Business- og Dropbox Education-kunder muligheten til å lagre filer (blokker) i EU. EU-basert fillagring tilbys på Amazon Web Services (AWS)-infrastruktur. For å lære mer om vår EU-infrastruktur, kontakt vår salgsavdeling.

Samarbeid for å beskytte personopplysningene dine

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

Imidlertid spiller brukerne også en nøkkelrolle i å beskytte personopplysningene sine. Dropbox lar deg konfigurere, bruke og overvåke kontoen din på måter som oppfyller organisasjonens personvern, sikkerhet og etterlevelsesbehov. Vår delte ansvarsveiledning 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 personopplysningene dine.

Oppsummering

Hver dag setter millioner av brukere sin lit til Dropbox. For å være verdig den tilliten, har vi utviklet og vil fortsette å utvide Dropbox med vekt på sikkerhet og personvern. Forpliktelsen vår til å beskytte brukernes personopplysninger er kjernen i hver beslutning vi tar. For mer informasjon, vennligst send en e-post til privacy@dropbox.com. For mer informasjon om GDPR, kan du også besøke GDPR veiledningssenteret vårt.