Dropbox

Privatliv og databeskyttelse

Indledning

Personlige data spiller en enorm rolle i samfundet og økonomien. I stigende grad søger folk større kontrol og klarhed over, hvordan deres personlige data bruges og beskyttes af organisationer, som de interagerer med.

Hos Dropbox er tillid fundamentet for vores forhold med millioner af mennesker og virksomheder verden over. Vi værdsætter den tillid, du har givet os, og tager ansvaret for at beskytte dine personlige data alvorligt.

Vores forpligtelser over for dig

Vi er forpligtet til at beskytte dine personlige data. Dropbox's Betingelser for brug skitserer dit ansvar, når du bruger vores tjenester. Vores Politik til beskyttelse af persondata beskriver vores forpligtelser til beskyttelse af personlige oplysninger overfor brugere og forklarer, hvordan vi indsamler, bruger og håndterer dine personlige data, når du bruger vores tjenester. Hvis du bor i Nordamerika (USA, Canada og Mexico), fungerer Dropbox, Inc. som din tjenesteudbyder.

For alle andre brugere fungerer Dropbox International Unlimited Company som registeransvarlig for dine personlige data.

Hvis du er bruger af Dropbox Business eller Dropbox Education, fungerer din organisation som dataansvarlig for alle personlige data, der leveres til Dropbox i forbindelse med din brug af Dropbox Business eller Dropbox Education. Den dataansvarlige bestemmer formålet og midlerne til behandling af personoplysninger. Dropbox fungerer som databehandleren, og behandler data på din organisations vegne, når du bruger Dropbox Business eller Dropbox Education, og vores erhvervs aftale i inkluderer forpligtelser relateret til databehandling og internationale dataoverførsler.

Vores resultater: Overholdelse

Om en tjeneste lever op til gældende standarder er en effektiv metode til at validere tjenestens troværdighed. Vi opfordrer og er glade for at give uafhængig verifikation af, at vores sikkerhed og praksis til beskyttelse af personlige oplysninger overholder de mest almindeligt accepterede standarder og forskrifter, såsom ISO 27001, ISO 27017, ISO 27018, HIPPA / HITECH, Tyskland BSI C5 og SOC 1, 2 og 3.

Desuden var vi en af de første leverandører af cloud-tjenester, der opnåede certificering med ISO 27018, den internationalt anerkendte standard til førende praksis inden for beskyttelse af cloudbaserede personlige oplysninger og andre data. Vores uafhængige tredjepartsrevisorer tester vores kontrol og leverer deres rapporter og udtalelser. Vi deler dem muligvis med dig, når det er muligt.

Bemærk, at mens omfanget af vores certificeringer og revisionsrapporter typisk henviser til Dropbox Business og Dropbox Education, er hovedparten af vores kontroller også gældende for brugere af Dropbox Basic, Plus og Professional. Mere information om de standarder, vi overholder, og hvordan vi verificerer vores praksis, findes på vores overholdelses web side.

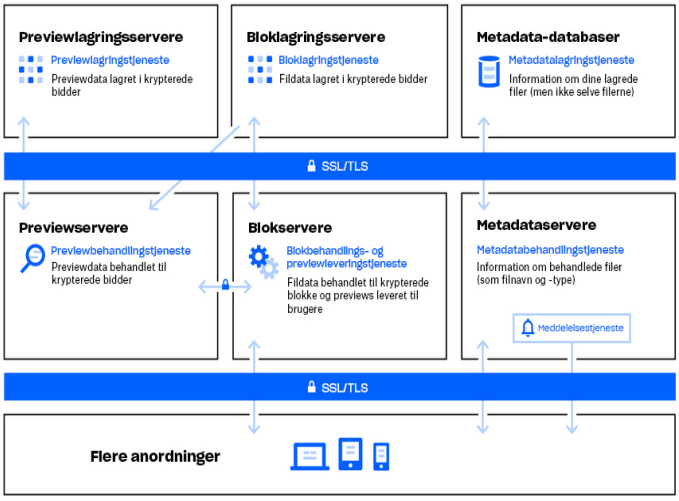
Dropbox

Dropbox-arkitektur: Beskyttelse af dine personlige data

Hos Dropbox tror vi på, at beskyttelsen af dine personlige data starter med at holde dine data sikre. Til dette formål er Dropbox designet med flere lag beskyttelse, herunder sikker filoverførsel, kryptering og applikationsniveau-kontroller, der er distribueret over en skalerbar, sikker infrastruktur.

Vores infrastruktur: Filer

Dropbox's infrastruktur til filer består af de komponenter, der er afbildet i nedenstående diagram.



Metadataservere

Visse grundlæggende oplysninger om brugerdata, kaldet metadata, opbevares i sin egen diskrete lagringstjeneste og fungerer som et indeks for dataene i brugernes konti. Metadata inkluderer grundlæggende konto- og brugeroplysninger, såsom e-mailadresse, navn og enhedsnavne. Metadata inkluderer også grundlæggende oplysninger om filer, herunder filnavne og typer, der hjælper med at understøtte funktioner som versionshistorik, gendannelse og synkronisering.

Databaser med metadata

Filmetadata gemmes i en MySQL-baseret databasetjeneste og afskærmes og replikeres efter behov for at imødekomme krav til ydelse og høj tilgængelighed.

Blokservere

Dropbox leverer en unik sikkerhedsmekanisme, der går ud over traditionel kryptering for at beskytte brugerdata. Blokservere behandler filer fra Dropbox-applikationer ved at opdele hver fil i blokke, kryptere hver filblok ved hjælp af en stærk kode og kun synkronisere blokke, der er ændret mellem revisioner. Når en Dropbox-applikation registrerer en ny fil eller ændres til en eksisterende fil, underretter applikationen blokservere om ændringen, og nye eller ændrede filblokke behandles og overføres til lagerserveren.

Bloklagerservere

Det faktiske indhold af brugernes filer gemmes i krypterede blokke med bloklagerservere. Før transmission opdeler Dropbox-klienten filer i filblokke som forberedelse til lagring. Bloklagerserveren fungerer som et CAS-system (Content-Addressable Storage), hvor hver enkelt krypteret filblok hentes baseret på dens hashværdi.

Forhåndsvisningsservere

Forhåndsvisningserverne er ansvarlige for at producere forhåndsvisning af filer. Forhåndsvisninger er en gengivelse af en brugers fil i et andet filformat, der er mere velegnet til hurtig visning på en slutbrugers enhed. Forhåndsvisningsservere henter filblokke fra bloklagerserverne for at generere forhåndsvisninger. Når der anmodes om en forhåndsvisning af en fil, henter forhåndsvisningsserverne den cachelagrede forhåndsvisning fra forhåndsvisningslagerserverne og overfører den til blokserverne. Forhåndsvisninger vises endeligt til brugerne af blokserverne.

Forhåndsvisningslagerservere

Cachelagrede forhåndsvisninger lagres i et krypteret format i forhåndsvisningslagerserverne.

Meddelelsestjeneste

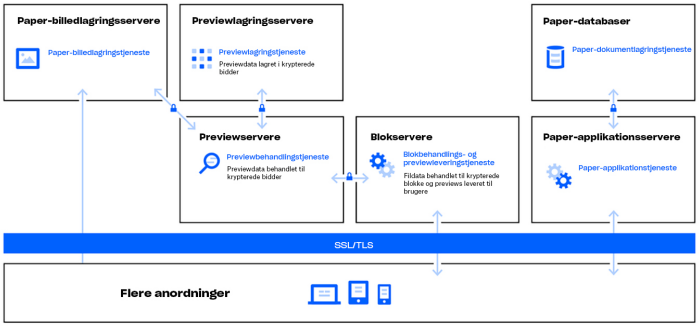
Denne separate tjeneste er dedikeret til at overvåge, om der er foretaget nogen ændringer i Dropbox-konti eller ej. Ingen filer eller metadata gemmes her eller overføres. Hver klient opretter en lang forespørgselsforbindelse til meddelelsestjenesten og venter. Når en ændring af en hvilken som helst fil i Dropbox finder sted, signalerer meddelelsestjenesten en ændring til den eller de relevante klienter ved at lukke den lange forespørgselsforbindelse. Lukning af forbindelsen signalerer, at klienten skal oprette forbindelse til metadata-servere for sikkert at synkronisere eventuelle ændringer.

For mere detaljeret information om Dropbox-sikkerhedsfunktioner og politikker kan du gennemgå Dropbox's hvidbog om erhvervssikkerhed eller kontakte sales@dropbox.com

Dropbox

Vores infrastruktur: Paper

Dropbox Paper (Paper) er en funktion i Dropbox-produktet. Paper bruger dog et for det meste tydeligt sæt systemer inden for Dropbox-infrastrukturmiljøet. Papers infrastruktur består af de komponenter, der er afbildet i diagrammet nedenfor .



Paper-applikationsservere

Paper-applikationsserverne behandler brugeranmodninger, gengiver outputtet af redigerede Paper-dokumenter for brugeren og udsender meddelelser. Paper-applikationsservere skriver indgående brugerredigeringer til Paper-databaserne, hvor de placeres i vedvarende opbevaring. Al kommunikation mellem Paper-applikationsservere og Paper-databaser krypteres med en stærk kode.

Paper-databaser

Det faktiske indhold i brugernes Paper-dokumenter såvel som visse metadata om disse Paper-dokumenter er krypteret i vedvarende lagring på Paper-databaserne. Det samme gælder oplysninger om de respektive Paper-dokumenter (f.eks. titel, delt medlemskab, tilladelser, projekt- og mappetilknytning osv.) samt indholdet i selve Paper-dokumenterne, herunder kommentarer og opgaver. Paper-databaserne partitioneres og reproduceres efter behov for at opfylde krav til ydeevne og høj tilgængelighed.

Paper-billedlagerservere

Inaktive billeder, der er uploadet til Paper-dokumenter, gemmes og krypteres på Paper-billedservere. Overførsel af billeddata mellem Paper-applikationen og Paper-billedservere sker via en krypteret session.

Forhåndsvisningsservere

Forhåndsvisningsserverne producerer forhåndsvisninger af både billeder, der er uploadet til Paper-dokumenter, samt hyperlinks, der er integreret i Paper-dokumenter. For billeder, der er uploadet til Paper-dokumenter, henter forhåndsvisningsserverne billeddata, der er gemt i Paper-billedlagerservere via en krypteret kanal. For hyperlinks, der er integreret i Paper-dokumenter, henter forhåndsvisningsserverne billeddataene og gengiver et eksempel på billedet ved hjælp af kryptering som specificeret af kildelinket. Forhåndsvisninger vises endeligt til brugerne af blokserverne.

Forhåndsvisningslagerservere

Paper bruger de samme forhåndsvisningslagerservere, der er beskrevet i Dropbox-infrastrukturdiagrammet til at gemme cache-forhåndsvisning af billeder. Cachelagrede forhåndsvisningsdele gemmes i et krypteret format i forhåndsvisningslagerservere.

Dropbox

Dropbox-kontrol: Vores interne praksis

Vi træffer omfattende foranstaltninger for at beskytte vores infrastruktur, netværk og applikationer. Nogle af de sikkerhedsforanstaltninger, vi har på plads, inkluderer kryptering i hvile, kryptering under transit og permanent sletning af filer.
Vi tilbyder også robust oplæring i beskyttelse af persondata og sikkerhed for alle vores medarbejdere for at opbygge en kultur, hvor det er en prioritet at være tillidsværdig.
Detaljer om nogle af vores kontroller er beskrevet nedenfor:

Uddannelse

En del af beskyttelsen af vores brugeres persondata involverer opbygning og vækst af en kultur med bevidsthed om sikkerhed og beskyttelse af personlige oplysninger. Dropbox-medarbejdere skal acceptere sikkerhedspolitikker, herunder en politik til beskyttelse af brugerdata, inden de får systemadgang. Kun medarbejdere med et specifikt behov har adgang til sådanne systemer.
Medarbejdere deltager også i obligatoriske kurser i sikkerhed og beskyttelse af personlige oplysninger på årsbasis.

Kryptering ved overførsel

For at beskytte fildata under transit mellem en Dropbox-klient (i øjeblikket computer, mobil, API eller web) og Dropbox's front-end-servere forhandles en krypteret forbindelse for at sikre sikker levering. Tilsvarende forhandles en krypteret forbindelse for at beskytte Paper dokumentdata under transit mellem en Paper-klient (i øjeblikket mobil, API eller web) og den hostede service. Disse forbindelser er krypteret ved hjælp af Secure Sockets Layer (SSL) / Transport Layer Security (TLS) for at skabe en sikker tunnel beskyttet af 128-bit eller højere kryptering med AES (Advanced Encryption Standard).

Kryptering ved inaktivitet

Filer, der er uploadet af brugere, lagres på Dropbox's lagerservere som diskrete filblokke. Hver blok er krypteret ved hjælp af 256-bit AES (Advanced Encryption Standard). Kun blokke, der er ændret mellem revisioner, synkroniseres. Tilsvarende krypteres Paper-dokumentdata, der er gemt på Paper-databaser, også i hvile ved hjælp af 256-bit AES (Advanced Encryption Standard).

Permanent sletning af filer og Paper-dokumenter

Når en Dropbox-bruger eller en administrator for et Dropbox Business- eller Dropbox Education-team markerer en fil til permanent sletning, udløser det en proces til permanent sletning af filen. Ligeledes, når en bruger eller en administrator af et Dropbox Business eller Dropbox Education-team markerer et Paper-dokument til permanent sletning, er der en lignende proces til permanent at slette Paper-dokumentdata og billeddata.

Anmodninger om adgang til personlige data

For adgang til personlige data ud over de filer og Paper-dokumenter, der er gemt med Dropbox, kan brugere logge på webstedet og gå til deres konto sider. Kontosiden viser oplysninger som navnet og e-mailadressen, der er knyttet til kontoen. Brugere kan også se IP-adresserne på tilsluttede sessioner, computere og mobile enheder samt apps, der er tilsluttet deres konti fra sikkerhedssiden og tilsluttet app side.

Dropbox-brugere har også mulighed for at anmode om adgang til eller sletning af andre personlige data, som Dropbox muligvis har samlet om dem.
Mere information om denne proces findes i Dropbox Hjælpe Center.

Fortrolighedsledelse hos Dropbox

Programteamet for beskyttelse af personlige oplysninger er ansvarligt for drift af Dropbox-programmet til beskyttelse af personlige oplysninger. Det implementerer vores vigtigste initiativer for beskyttelse af personlige data og fører an med beskyttelse af personlige oplysninger i vores datalivscyklus. Dropbox-programmet til beskyttelse af personlige oplysninger er også støttet af adskillige tværfunktionelle juridiske underhold. Disse underhold giver den ekstra ekspertise, der kræves for at betjene og føre tilsyn med de daglige opgaver i programmet til beskyttelse af personlige oplysninger.

DPO-teamet fungerer adskilt fra de andre funktioner til beskyttelse af persondata og fungerer som overholdelse og overvågning af persondata, direkte støtte af databeskyttelsesrådgiveren i udførelsen af deres opgaver. Data Protection Officer (DPO, databeskyttelsesrådgiver) er EU's lokale repræsentant og kan kontaktes på privacy@dropbox.com.

Dropbox

Principper for dataanmodninger fra myndighederne

Vi forstår, at når brugerne overdrager os deres personlige data, forventer de, at vi holder disse data fortrolige. Som de fleste onlinetjenester modtager Dropbox undertiden anmodninger fra myndigheder, der søger information om sine brugere.

Principperne herunder beskriver, hvordan vi håndterer de dataanmodninger, vi modtager fra myndigheder.

Udvise gennemsigtighed

Vi mener, at 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. Gennemsigtighed i den forbindelse styrker brugerne, fordi de får større indsigt i tilfælde og mønstre for hvordan myndigheder blander sig. Vi fortsætter både med at offentliggøre detaljerede oplysninger om disse anmodninger og arbejder for vores ret til at offentliggøre flere af disse vigtige oplysninger.

Bekæmp vidtgående anmodninger

Dataanmodninger fra myndigheder skal være begrænset i de oplysninger, de søger, og snævert tilpasset specifikke personer og legitime undersøgelser. Vi vil opponere imod generelle og alt for brede anmodninger.

Levere tjenester, man kan have tillid til

Myndigheder bør aldrig installere bagdøre til online tjenester eller kompromittere infrastrukturen for at indhente brugerdata. Vi vil fortsætte med at 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 forsyner folk med forskellige beskyttelsesniveauer, ud fra hvor de bor eller deres statsborgerskab, er forældede og afspejler ikke onlinetjenesters globale natur. Vi vil fortsætte med at være fortalere for ændringer af disse love.

Disse principper sammen med vores årlige gennemsigtighedsrapport offentliggøres på Dropbox-webstedet: https: // www.dropbox.com/transparency.

Yderligere oplysninger om vores kontroller og vores tilgang til beskyttelse af dine personlige data kan ses i vores Dropbox hvidbog som erhvervssikkerhed.

Andre, der arbejder for og med Dropbox

Dropbox administrerer størstedelen af aktiviteter knyttet til levering af vores tjenester; dog bruger vi nogle betroede tredjeparter i forbindelse med vores tjenester (for eksempel udbydere 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 til beskyttelse persondata, og vi forbliver ansvarlige for deres håndtering af dine oplysninger i overensstemmelse med vores instruktioner.

Hver tredjepart gennemgår en streng kontrolproces, herunder sikkerhedsgennemgang og regelmæssige kontraktlige anmeldelser, for at evaluere deres evne til at opfylde vores forpligtelser til databeskyttelse.

Internationale dataoverførsler

Dropbox bruger en række juridiske mekanismer til internationale overførsler af personoplysninger fra EU til USA. Vi er certificeret i henhold til EU-USA og Schweiz-USA programmer for privatlivsskjold angående beskyttelse, brug og tilbageholdelse af persondata og dettes overførsel fra EU og Schweiz til USA. Ud over privatlivsskjold levere Dropbox også stærke kontraktmæssige garantier omkring beskyttelse af persondata for sine tjenester og har implementeret EU-modelkontraktklausuler til at dække sine internationale overførsler af data.

Dropbox

GDPR: Den almindelige databeskyttelsesforordning

Den almindelige databeskyttelsesforordning, eller GDPR, er en EU-forordning, der fastlægger en juridisk ramme til beskyttelse af personoplysninger fra dataregistrerede i EU.

GDPR er det mest betydningsfulde stykke europæisk databeskyttelseslovgivning siden EU's databeskyttelsesdirektiv fra 1995, og mange virksomheder – inklusive Dropbox – der driver forretning i Europa har investeret kraftigt i GDPR-overholdelse.

GDPR harmoniserer databeskyttelseslove overalt i Europa og bringer dem op med den hurtige teknologiske ændring, der er sket i de sidste to årtier.

Det bygger på tidligere juridiske rammer i EU, herunder EU's databeskyttelsesdirektiv, og indfører nye forpligtelser og ansvar for organisationer, der håndterer personoplysninger, samt nye rettigheder for enkeltpersoner med hensyn til deres personoplysninger.

personlige data. Organisationer, der er etableret i EU, såvel som organisationer, der behandler personoplysninger om EU-registrerede, er forpligtet til at overholde GDPR.

Dropbox' vej til overholdelse af GDPR

Dropbox er forpligtet til at overholde GDPR. Respekten for persondata og sikkerhed blev indbygget i vores virksomhed fra begyndelsen, og efterhånden som vi er vokset, har vores fokus på håndtering og beskyttelse af de data, som vores brugere overdrager os, været en prioritet. Dropbox holder sig foran overholdelseskurven –som beskrevet ovenfor var vi en af de første cloud-tjenesteudbydere, som opnåede ISO 27018-certificering for vores erhvervsbrugere. Grundet dette stærke fundament betragter Dropbox GDPR-overholdelse som en udbygning af vores nuværende praksis og kontroller og repræsenterer et løbende, udviklende sæt af initiativer for at sikre, at vores brugeres persondata altid er beskyttede.

Dropbox' vej mod overholdelse begyndte, så snart forordningen blev indført i 2016. Vores første skridt var at danne et tværfunktionelt team af specialister inden for databeskyttelse, bestående af juridisk rådgivning, teknikere inden for sikkerhed og overholdning, ingeniører inden for produkter og infrastrukturer. Vores team afsluttede derefter en fuld vurdering af vores nuværende sikkerheds- og databeskyttelsespraksis i forhold til GDPR-kravene.

Vores næste skridt var at udføre en evaluering af vores personlige databehandlingsaktiviteter og spore livscyklussen for persondata gennem vores systemer. Disse øvelser betegnes undertiden som udførelse af datakortlægning og udførelse af vurderinger af databeskyttelsens effekt.

datakortlægning og udførelse af vurderinger af databeskyttelsens effekt.

Siden da har vi fortsat med at bygge videre på vores eksisterende interne processer og procedurer for at sikre, at vi overholder ansvarlighedsprincipperne under GDPR-kravene. Dette er vigtigt, da GDPR sætter øget fokus på dokumentering af beslutninger og praksisser, der påvirker personlige data.

Dropbox

Vi støtter vores brugere på deres GDPR-rejser

Dropbox har kontrol- og synlighedsfunktioner, der kan hjælpe dig med nemmere administration af dine databeskyttelsesforpligtelser, herunder GDPR-overholdelsesforpligtelser. Selvfølgelig begynder eller slutter GDPR-overholdelse på tværs af din organisation ikke med forholdet til dine leverandører, såsom Dropbox. Selv om vores funktioner kan hjælpe dig med at styre dine forpligtelser, kan de ikke sikre overholdelse i og af sig selv. GDPR-overholdelse kræver større overvejelser om, hvordan data bevæger sig rundt og beskyttes i din organisation. Hver organisation skal tage sine egne skridt for at nå overensstemmelse med leverandører som vigtige partnere på denne rejse.

Dataminimering

Et vigtigt element i GDPRs krav til beskyttelse af persondata er, at organisationer skal designe deres tjenester på en data-minimerende måde. Dette betyder at have god synlighed og kontrol over dataene i din organisation for at hjælpe dig med at administrere dem. Dropbox Business dashboard for administratorer er et nyttigt værktøj til at hjælpe med dette, da det giver dig mulighed for at overvåge teamaktivitet, se tilsluttede enheder og revisionsdelingsaktivitet. Vi arbejder for at integrere Privacy by Design-principperne i nye produkter og funktioner.

Beskyttelse og gendannelse af data

Mistet enhedsbeskyttelse, versionshistorik og gendannelse af filer kan hjælpe med at beskytte mod utilsigtet tab, beskadigelse eller ødelæggelse af personlige data og kan hjælpe med muligheden for at gendanne tilgængelighed og adgang til personlige data rettidigt i tilfælde af en hændelse. To-faktor-godkendelse er en anden vigtig foranstaltning, som vi opfordrer til for at hjælpe med at beskytte dine data.

Journalføring

GDPR øger også forpligtelserne for organisationer om detaljeret journalføring af deres behandlingsaktiviteter. Vores revisions -og aktivitetslogfiler kan hjælpe dig med bedre at forstå dine behandlingsaktiviteter til støtte for din journalføring.

Adgangsadministration

I Dropbox Business dashboard for administratorer administrerer du nemt teammedlemmers adgang til filer, mapper og Paper-dokumenter. For delte fillink giver vores linktilladelsesfunktion dig mulighed for at beskytte de delte links med adgangskode, indstille udløbsdatoer for at give midlertidig adgang og begrænse adgangen til personer i din organisation. I tilfælde af, at ansvaret ændres mellem brugere, kan du med vores kontooverførselsværktøj nemt overføre filer og ejerskab af Paper-dokumenter fra en bruger til en anden.

Administratorer har også mulighed for at deaktivere en brugers adgang til deres konto, mens de bevarer deres data -og deleforhold for at holde din organisations oplysninger sikre. Til sidst: Fjernsletningsfunktionen har du mulighed for at rydde filer og Paper-dokumenter fra mistede eller stjålne enheder.

EU-infrastruktur

Mens GDPR ikke kræver, at persondata skal hostes i 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. Lær mere om vores EU-infrastruktur ved at kontakte vores salgs team.

Dropbox

Samarbejde for at beskytte dine persondata

Dropbox arbejder med sine brugere for at beskytte deres persondata. Vi træffer omfattende foranstaltninger for at beskytte vores infrastruktur, netværk og applikationer, uddanne medarbejdere i sikkerhed og praksisser til beskyttelse af persondata, opbygning en kultur, hvor det er højst prioriteret at være tillidsværdig, og sætte vores systemer og praksis gennem streng tredjeparts test og revision.

Brugere spiller imidlertid også en vigtig rolle i beskyttelsen af deres persondata. Dropbox giver dig mulighed for at konfigurere, bruge og overvåge din konto på måder, der imødekommer din organisations behov for beskyttelse af persondata, sikkerhed og overholdelse. Vores guide om delt ansvar kan hjælpe dig med at forstå mere om, hvad vi gør for at holde din konto sikker, og hvad du kan gøre for at bevare synligheden og kontrollen over dine persondata.

Resumé

Hver dag stoler millioner af brugere Dropbox. For at være værdig til denne tillid, bygger og udvikler vi fortsat Dropbox med vægt på sikkerhed og beskyttelse af persondata. Vores forpligtelse til at beskytte vores brugeres persondata er kernen i hver beslutning, vi træffer. For mere information kan du kontakte privacy@dropbox.com. For mere information om GDPR kan du også besøge vores GDPR vejlednings center.