Dropbox

# Privacy- en gegevens-bescherming

## Inleiding

Persoonsgegevens spelen een grote rol in de maatschappij en de economie. In toenemende mate willen mensen meer controle en duidelijkheid over de manier waarop hun persoonsgegevens worden gebruikt en beschermd door organisaties waar ze mee werken. Tegelijkertijd eisen mensen dat organisaties duidelijke instructies krijgen voor het beschermen van persoonsgegevens.

Bij Dropbox staat vertrouwen aan de basis van onze relatie met miljoenen mensen en bedrijven overal ter wereld. We waarderen het vertrouwen dat je in ons hebt gesteld en nemen de verantwoordelijkheid voor het beschermen van jouw persoonsgegevens serieus.

## Onze belofte aan jou

Wij doen onze uiterste best om jouw persoonsgegevens te beschermen. In de Servicevoorwaarden van Dropbox worden jouw verantwoordelijkheden beschreven wanneer je onze service gebruikt. In ons Privacybeleid staat welke verplichtingen wij hebben voor de privacy van gebruikers en leggen we uit hoe we jouw persoonsgegevens verzamelen, gebruiken en verwerken wanneer je onze service gebruikt. Als je ingezetene van de Europese Unie (EU) bent, worden je gegevens geregeld door Dropbox International Unlimited Company, gevestigd in Ierland.

Als je Dropbox Business of Dropbox Education gebruikt, fungeert jouw organisatie als datacontroller voor alle persoonsgegevens die Dropbox ontvangt in verband met jouw gebruik van Dropbox Business of Dropbox Education. De datacontroller bepaalt het doel en de middelen van het verwerken van persoonsgegevens. Dropbox fungeert als dataprocessor en verwerkt gegevens namens je organisatie wanneer je Dropbox Business of Dropbox Education gebruikt. In onze Overeenkomst voor Business staan verplichtingen met betrekking tot de verwerking van gegevens en internationale gegevensoverdracht.

## Onze reputatie: naleving

Naleving is een effectieve manier om de betrouwbaarheid van een service te valideren. We stimuleren het aan bieden van (en leveren zelf ook) onafhankelijke verificatie dat onze beveiligings- en privacypraktijken voldoen aan de breedst geaccepteerde standaarden en reguleringen, zoals ISO 27001, ISO 27017, ISO 27018, Germany BSI C5 en SOC 1, 2 en 3. We waren bijvoorbeeld een van de eerste cloudserviceproviders die voor ISO 27018 zijn gecertificeerd, de internationaal erkende standaard voor toonaangevende praktijken in cloudprivacy en gegevensbescherming. Onze onafhankelijke externe auditors testen onze functies en geven ons hun rapporten en meningen. We zullen deze waar mogelijk met je delen.

Let op: hoewel de strekking van onze certificeringen en auditrapporten doorgaans verwijzen naar Dropbox Business en Dropbox Education, gelden de meeste van onze bedieningselementen ook voor gebruikers van Dropbox Basic, Plus en Professional. Ga naar onze webpagina over naleving voor meer informatie over de standaarden waaraan wij voldoen en hoe we onze praktijken verifiëren.

Lees voor meer informatie over de beveiligingsfuncties en -beleidsregels de whitepaper over beveiliging van Dropbox Business of neem contact op met sales@dropbox.com

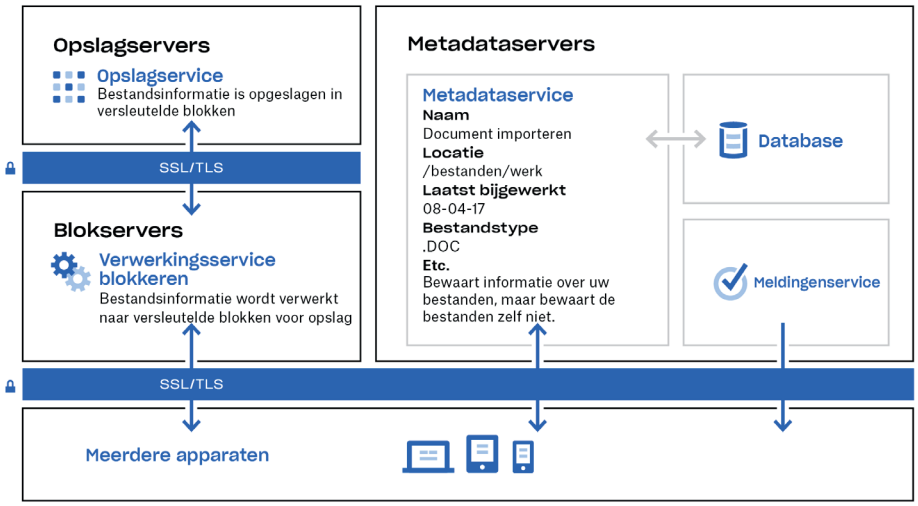
Dropbox

# Dropbox-architectuur: jouw persoonsgegevens beschermen

We zijn ervan overtuigd dat bescherming van persoonsgegevens begint bij het beveiligen van je gegevens. Dropbox is daarom opgebouwd met meerdere beveiligingslagen, zoals veilige bestandsgegevensoverdracht, versleuteling en functies op toepassingsniveau, die over een schaalbare, beveiligde infrastructuur zijn verspreid.

## Onze infrastructuur: bestanden

De Dropbox-infrastructuur voor bestanden bestaat uit de onderdelen die je in het onderstaande diagram ziet staan.




## Blokservers

Standaard biedt Dropbox een uniek beveiligingsmechanisme voor de bescherming van gebruikersgegevens dat verdergaat dan traditionele versleuteling. Blokservers verwerken bestanden van de Dropbox-toepassingen door elk bestand in blokken te verdelen, elk bestandsblok te versleutelen met een sterke coderingsmethode en alleen de blokken te synchroniseren die tussen revisies in zijn aangepast. Wanneer een Dropbox-toepassing een nieuw bestand ontdekt of detecteert dat er iets aan een bestaand bestand is gewijzigd, brengt de toepassing de Blokservers op de hoogte van die verandering en worden nieuwe of aangepaste bestandsblokken verwerkt en verzonden naar de Opslagservers.

## Meldingsservice

Deze afzonderlijke service houdt zich bezig met het controleren op wijzigingen aan Dropbox-accounts. Hier worden geen bestanden of metagegevens opgeslagen of verzonden. Elke client brengt een 'long poll'-verbinding tot stand met de meldingsservice en wacht. Bij een verandering aan een bestand in Dropbox geeft de meldingsservice een wijziging door aan de relevante client(en) door de long poll-verbinding te sluiten. Het sluiten van de verbinding is een signaal dat de client een veilige verbinding moet maken met de Metagegevensservers om wijzigingen te synchroniseren.

## Servers met metagegevens

Bepaalde elementaire informatie die wordt aangeduid als metagegevens, wordt bewaard in een eigen afgezonderde opslagservice en fungeert als een index voor de gegevens in gebruikersaccounts. Dropbox-metagegevens worden opgeslagen in een MySQL-databaseservice, en worden waar nodig opgesplitst en gerepliceerd om te kunnen voldoen aan de vereisten op het gebied van prestaties en hoge beschikbaarheid. Metagegevens zijn onder meer basisgegevens over accounts en gebruikers, zoals e-mailadres, naam en namen van apparaten. Onder metagegevens vallen ook basisgegevens over bestanden, waaronder bestandsnamen en -typen, waarmee functies zoals versiegeschiedenis, herstel en synchronisatie worden ondersteund.

## Opslagservers

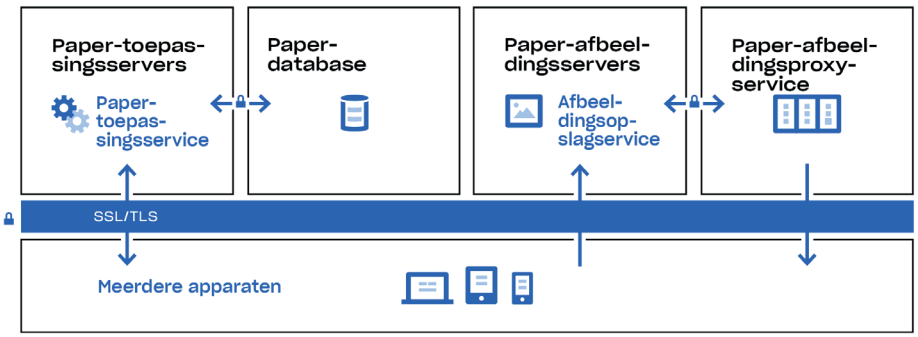
Zodra bestanden in blokken zijn opgesplitst en door de Blokservers zijn versleuteld, wordt de daadwerkelijke inhoud van deze bestandsblokken opgeslagen in de Opslagservers. De Opslagservers fungeren als een CAS-systeem, wat staat voor Content-Addressable Storage, waarbij elk afzonderlijk versleuteld bestandsblok wordt opgehaald aan de hand van de hash-waarde.

Lees voor meer informatie over de beveiligingsfuncties en -beleidsregels de whitepaper over beveiliging van Dropbox Business of neem contact op met sales@dropbox.com

Dropbox

## Onze infrastructuur: Paper

Dropbox Paper (Paper) is een functie van het Dropbox-product. Paper gebruikt echter een andere set systemen in de omgeving van de Dropbox-infrastructuur. De Paper-infrastructuur bestaat uit de onderdelen die je in het onderstaande diagram ziet staan.




### Paper-toepassingsservers

De Paper-toepassingsservers verwerken gebruikersverzoeken, geven de uitvoer van bewerkte Paper-documenten terug aan de gebruiker en voeren meldingsdiensten uit. Paper-toepassingsservers schrijven inkomende gebruikersbewerkingen naar de Paper-databases, waar ze in permanente opslag worden geplaatst. Communicatiesessies tussen de Paper-toepassingsservers en Paper-databases worden gecodeerd met een sterke sleutel.

### Paper-afbeeldingsproxyservice

De Paper-afbeeldingsproxyservice levert voorbeelden van afbeeldingen zowel voor afbeeldingen die naar Paper-documenten zijn geüpload als hyperlinks die in Paper-documenten zijn ingesloten. Voor afbeeldingen die naar Paper-documenten zijn geüpload, haalt de Paper-afbeeldingsproxyservice via een gecodeerd kanaal afbeeldingsgegevens op die zijn opgeslagen in de Paper-afbeeldingsservers. Voor hyperlinks die in Paper-documenten zijn ingesloten, haalt de afbeeldingsproxyservice uit de bronkoppeling afbeeldingsgegevens op en wordt een voorbeeld van de afbeelding weergegeven met HTTP of HTTPS zoals door de bronlink opgegeven.

### Paper-databases

De daadwerkelijke inhoud van Paper-documenten van gebruikers, evenals bepaalde metagegevens van deze Paper-documenten, worden gecodeerd in permanente opslag in de Paper-databases. Dit omvat informatie over een Paper-document (zoals de titel, gedeeld abonnement en machtigingen, project- en mapkoppelingen en andere informatie), evenals inhoud binnen het Paper-document zelf, waaronder opmerkingen en taken. De Paper-databases worden waar nodig opgesplitst en gerepliceerd om te kunnen voldoen aan de vereisten op het gebied van prestaties | en hoge beschikbaarheid.

### Paper-afbeeldingservers

Afbeeldingen geüpload naar Paper-documenten worden opgeslagen en in rust gecodeerd op de Paper-afbeeldingsservers. Verzending van gegevens van afbeeldingen tussen de Paper-toepassing en Paper-afbeeldingsservers vindt plaats via een gecodeerde sessie.

Dropbox

# Dropbox-functies: onze interne praktijken

We nemen uitvoerige maatregelen om onze infrastructuur, ons netwerk en onze toepassingen te beschermen, werknemers te trainen op het gebied van beveiligings- en privacymethoden en een cultuur op te zetten waar betrouwbaarheid de hoogste prioriteit heeft. Hieronder worden enkele functies beschreven:

### Training

Onderdeel van het beschermen van de persoonsgegevens van onze gebruikers is het tot stand brengen en uitbreiden van een cultuur waarin mensen zich bewust zijn van beveiliging en privacy. Dropbox-werknemers moeten verplicht akkoord gaan met het beveiligingsbeleid, waaronder een privacybeleid voor gebruikersgegevens, om toegang tot systemen te krijgen. Werknemers nemen ook deel aan verplichte beveiligings- en privacytrainingen voor nieuwe werknemers, alsmede jaarlijkse follow-uptrainingen. Daarnaast krijgen werknemers regelmatig bewustheidstrainingen door informatieve e-mails, gesprekken, presentaties en resources die via ons intranet beschikbaar zijn.

### Versleuteling tijdens verzending

Om bestandsgegevens tijdens de verzending van een Dropbox-client (momenteel desktop, mobiel, API of web) naar de front-endservers te beschermen, wordt er een versleutelde verbinding tot stand gebracht om een veilige levering te garanderen. Evenzo wordt een versleutelde verbinding tot stand gebracht om Paper-documentgegevens te beschermen die worden overgebracht van een Paper-client (momenteel mobiel, API of web) naar de gehoste service. Deze verbindingen zijn versleuteld met behulp van Secure Sockets Layer (SSL)/ Transport Layer Security (TLS) om een veilige tunnel te creëren die door 128-bits (of hogere) AES-versleuteling (Advanced Encryption Standard) wordt beveiligd.

### Versleuteling tijdens inactiviteit

Bestanden die door gebruikers zijn geüpload, worden als discrete bestandsblokken opgeslagen op de Opslagservers van Dropbox. Elk blok wordt versleuteld met 256-bits AES (Advanced Encryption Standard). Alleen blokken die tussen twee revisies in zijn aangepast, worden gesynchroniseerd. Evenzo worden Paper-documentgegevens die in Paper-databases zijn opgeslagen, versleuteld tijdens inactiviteit met 256-bits AES (Advanced Encryption Standard).

### Definitieve verwijdering van bestanden en Paper-documenten

Wanneer een Dropbox-gebruiker, of de beheerder van een Dropbox Business- of Dropbox Education-team, een bestand markeert voor definitieve verwijdering, wordt een proces geactiveerd om het bestand definitief te verwijderen. Evenzo wordt een vergelijkbaar proces voor definitieve verwijdering van Paper-documentgegevens en afbeeldingsgegevens geactiveerd wanneer een gebruiker, of de beheerder van een Dropbox Business- of Dropbox Education-team, een Paper-document voor definitieve verwijdering markeert.

### Toegangsverzoeken tot persoonsgegevens

Voor informatie over andere zaken dan de bestanden en Paper-documenten die in Dropbox zijn opgeslagen, kunnen gebruikers zich aanmelden op de website en hun accountpagina's openen. Op de accountpagina staat informatie zoals de naam en het e-mailadres die aan het account zijn gekoppeld. Gebruikers kunnen tevens de IP-adressen zien van verbonden sessies, computers en mobiele apparaten, en apps die met hun accounts zijn verbonden. Hiervoor openen ze de beveiligingspagina en de pagina met verbonden apps.

Dropbox-gebruikers hebben ook de mogelijkheid om een verzoek in te dienen voor toegang tot of de verwijdering van andere persoonsgegevens die we mogelijk over hen hebben verzameld. Ga voor meer informatie over dit proces naar het Helpcentrum van Dropbox.

Dropbox

### Principes voor aanvragen van overheidsgegevens

Wanneer gebruikers ons hun persoonsgegevens toevertrouwen, begrijpen we dat zij van ons verwachten deze vertrouwelijk te houden. Net zoals de meeste onlineservices krijgt Dropbox soms verzoeken van overheden die informatie over hun gebruikers zoeken.

Lees in de onderstaande principes hoe wij ontvangen gegevensverzoeken van overheden verwerken.

### Transparant zijn

Wij vinden dat online services het aantal en het type overheidsverzoeken die worden ontvangen, moeten kunnen publiceren en dat personen geïnformeerd moeten worden wanneer informatie over hen is aangevraagd. Zulke transparantie stelt gebruikers in staat om instanties en patronen van overmacht van de overheid beter te begrijpen. We blijven gedetailleerde informatie over deze verzoeken publiceren en pleiten voor het recht om meer van deze belangrijke informatie te verstrekken.

### Strijden tegen zeer brede verzoeken

Gegevensverzoeken van overheden moeten worden beperkt in het soort informatie dat ze zoeken en uitsluitend zijn toegespitst op specifieke personen en legitieme onderzoeken. We strijden tegen bulkverzoeken en brede verzoeken.

### Vertrouwde diensten aanbieden

Overheden mogen nooit in het geheim installaties uitvoeren in online services of de infrastructuur misbruiken om gebruikersgegevens te verkrijgen. We werken voortdurend aan de beveiliging van onze systemen en blijven ons inzetten voor wetswijzigingen om duidelijk te maken dat dit soort activiteiten illegaal is.

### Alle gebruikers beschermen

Wetten die mensen verschillende bescherming bieden op basis van waar ze wonen of hun burgerschap zijn verouderd en weerspiegelen niet het wereldwijde karakter van online diensten. We zullen blijven pleiten voor de hervorming van deze wetten.

Deze principes worden, in combinatie met ons jaarverslag op het gebied van transparantie, openbaar gemaakt op de Dropbox-website: https://www.dropbox.com/transparancy.

Voor meer informatie over onze functies en onze kijk op de bescherming van uw persoonsgegevens, kunt u onze Dropbox Business-whitepaper over beveiliging raadplegen.

## Anderen die voor Dropbox werken

Dropbox beheert het merendeel van de activiteiten met betrekking tot de inrichting van onze services; we maken echter soms gebruik van vertrouwde externe partijen met betrekking tot onze services (bijvoorbeeld leveranciers van klantenondersteuning en IT-services). Deze externe partijen hebben alleen toegang tot je gegevens om namens ons en in overstemming met ons Privacybeleid taken uit te voeren. Wij blijven verantwoordelijk voor hun verwerking van jouw gegevens conform onze instructies. Elke externe partij wordt onderworpen aan een rigoreus screeningproces, inclusief beveiligingsbeoordelingen en regelmatige contractuele beoordelingen, zodat we kunnen evalueren of ze aan onze verplichtingen inzake gegevensbescherming kunnen voldoen.

## Internationale gegevensoverdracht

Dropbox vertrouwt op diverse juridische mechanismen voor hun internationale overdracht van persoonsgegevens van de EU naar de Verenigde Staten. We zijn gecertificeerd volgens de Privacy Shield Programs tussen de EU en de VS en tussen Zwitserland en de VS met betrekking tot het verzamelen, gebruiken en bewaren van persoonsgegevens en de overdracht daarvan van de EU en Zwitserland naar de Verenigde Staten. Naast het Privacy Shield biedt Dropbox krachtige contractuele garanties rondom de privacy van onze services. Voor de dekking van onze internationale gegevensoverdrachten vertrouwen we op modelcontractclausules van de EU.

Dropbox

# GDPR: de Algemene verordening gegevensbescherming

De GDPR, ook wel de Algemene verordening gegevensbescherming of AVG genoemd, is een EU-verordening die een nieuw juridisch kader vaststelt ter bescherming van de persoonsgegevens van EU-ingezetenen. De GDPR is het belangrijkste onderdeel van de Europese wetgeving inzake gegevensbescherming sinds de Europese gegevensbeschermingsrichtlijn van 1995, en veel bedrijven, waaronder Dropbox, die handelen met bedrijven in Europa, hebben veel geïnvesteerd in naleving van deze verordening.

De GDPR is erop gericht wetgeving uit heel Europa op het gebied van gegevensbescherming op elkaar af te stemmen en geschikt te maken voor de snelle technologische veranderingen die we de afgelopen twintig jaar hebben gezien. De nieuwe wet is gebaseerd op oude juridische kaders in de EU, waaronder de Europese gegevensbeschermingsrichtlijn, en introduceert nieuwe verplichtingen en verantwoordelijkheden voor organisaties die persoonsgegevens verwerken, maar ook nieuwe rechten voor personen met betrekking tot hun persoonsgegevens. Organisaties die in de EU zijn gevestigd, alsmede organisaties die persoonsgegevens van ingezetenen van de EU verwerken, moeten verplicht voldoen aan de GDPR.

# Het GDPR-nalevingsproces van Dropbox

Dropbox streeft naar volledige naleving van de GDPR. Al vanaf het begin vormen privacy en beveiliging de hoeksteen van ons bedrijf, en hoe groot we ook zijn gegroeid: het verwerken en beschermen van de gegevens die gebruikers aan ons toevertrouwen heeft nog steeds de hoogste prioriteit. Dropbox heeft een reputatie hoog te houden op het gebied van naleving. Zoals we hierboven al schrijven, waren wij een van de eerste cloudserviceproviders die een ISO 27018-certificering voor onze zakelijke klanten hebben behaald. Gezien deze sterke basis beschouwt Dropbox naleving van de GDPR als logische volgende stap voor onze bestaande praktijken en functies.

Het proces van Dropbox voor naleving van de GDPR begon al in 2016, toen de verordening werd aangenomen. De eerste stap was het vormen van een team uit alle gelederen, met specialisten op het gebied van gegevensbescherming, zoals juridisch adviseurs, beveiligingsexperts en nalevingsprofessionals, maar ook product- en infrastructuurengineers. Vervolgens voerde het team een volledige evaluatie van onze huidige beveiligings- en gegevensbeschermingspraktijken uit, met de GDPR-vereisten als basis. Ten tweede moest een evaluatie worden uitgevoerd van onze activiteiten op het gebied van de verwerking van persoonsgegevens. Ook werd de levenscyclus van persoonsgegevens door onze systemen gecontroleerd. Dit wordt ook wel het uitvoeren van gegevenstoewijzingen en het voltooien van impactbeoordelingen voor gegevensbescherming genoemd.

Sindsdien zijn we verdergegaan met het uitbreiden van onze bestaande interne processen en procedures, om te garanderen dat we voldoen aan de aansprakelijkheidsprincipes van de GDPR-vereisten. Dit is van belang omdat de GDPR sterk is gericht op het documenteren van beslissingen en praktijken die invloed op persoonsgegevens hebben.

Dropbox

# Onze gebruikers helpen bij hun GDPR-processen

Dropbox biedt controle- en zichtbaarheidsfuncties waarmee je gemakkelijker je verplichtingen omtrent gegevensbescherming kunt beheren, waaronder GDPR-nalevingseisen. Natuurlijk staat of valt GDPR-naleving in je organisatie niet bij de relatie met bepaalde leveranciers zoals Dropbox. Hoewel onze functies je kunnen helpen om je verplichtingen te beheren, kunnen ze de naleving zelf niet garanderen. Voor GDPR-naleving moet je in bredere zin nadenken over de manier waarop gegevens rondgaan en worden beschermd in je organisatie. Elke organisatie moet zelf stappen zetten om naleving tot stand te brengen. Leveranciers zijn in dat proces waardevolle partners.

### Minimalisatie van gegevens

Een belangrijk onderdeel van de nieuwe GDPR-vereiste voor Privacy by Design is dat organisaties hun services zodanig moeten ontwerpen dat de hoeveelheid gegevens wordt geminimaliseerd. Dit houdt in dat de gegevens in je organisatie goed zichtbaar moeten zijn en goed kunnen worden gecontroleerd, zodat je ze eenvoudig kunt beheren. Het Dropbox-beheerdashboard is hiervoor een handig hulpprogramma, omdat je hiermee je teamactiviteit kunt bijhouden, verbonden apparaten kunt weergeven en deelactiviteiten kunt beoordelen.

### Bescherming en herstel van gegevens

Functies voor bescherming van verloren apparaten, versiegeschiedenis en bestandsherstel beschermen tegen onbedoeld verlies, beschadiging of vernietiging van persoonsgegevens en helpen met de mogelijkheid om tijdig beschikbaarheid van en toegang tot persoonsgegevens te herstellen in het geval van een incident. Verificatie met twee factoren is een andere belangrijke maatregel die we aanbevelen om je gegevens te helpen beschermen.

### Records bijhouden

De GDPR legt ook meer verplichtingen op aan organisaties voor het bewaren van gedetailleerde records van hun verwerkingsactiviteiten. Met behulp van onze controle- en activiteitenlogboeken begrijp je beter hoe je verwerkingsactiviteiten werken, ter ondersteuning van het bewaren van records.

### Toegangsbeheer

Via het Dropbox-beheerdashboard kun je eenvoudig toegang voor teamleden tot bestanden, mappen en Paper-documenten beheren. Voor links naar gedeelde bestanden kun je via onze functie voor linkmachtigingen de gedeelde links beveiligen met een wachtwoord, vervaldatums instellen voor tijdelijke toegang en de toegang beperken tot alleen mensen binnen je organisatie. In het geval verantwoordelijkheden tussen gebruikers veranderen, kun je met ons hulpprogramma voor accountoverdracht eenvoudig bestanden en eigendom van Paper-documenten overdragen van de ene naar de andere gebruiker. Beheerders hebben bovendien de mogelijkheid de toegang van een gebruiker tot een account te ontzeggen terwijl de gegevens en instellingen voor delen worden behouden om zo de informatie van je bedrijf veilig te houden. Als laatste kun je met de functie voor extern verwijderen bestanden en Paper-documenten van verloren of gestolen apparaten verwijderen.

### EU-infrastructuur

In de meeste gevallen is het voor de GDPR niet verplicht om persoonsgegevens te hosten binnen de EU, maar Dropbox biedt gekwalificeerde gebruikers van Dropbox Business en Dropbox Education wel de mogelijkheid om bestanden (blokken) in de EU op te slaan. Bestandsopslag dat in de EU is gevestigd wordt aangeboden via de AWS-infrastructuur (Amazon Web Services). Voor meer informatie over onze EU-infrastructuur kun je contact opnemen met ons verkoopteam.

Lees voor meer informatie over de beveiligingsfuncties en -beleidsregels de whitepaper over beveiliging van Dropbox Business of neem contact op met sales@dropbox.com

Dropbox

# Samenwerken aan de bescherming van je persoonsgegevens

Dropbox werkt samen met hun gebruikers om hun persoonsgegevens te beschermen. We nemen uitvoerige maatregelen om onze infrastructuur, ons netwerk en onze toepassingen te beschermen, werknemers te trainen op het gebied van beveiligings- en privacymethoden, een cultuur op te zetten waar betrouwbaarheid de hoogste prioriteit heeft en onze systemen en methoden op rigoureuze wijze te laten testen en controleren door derden.

Gebruikers spelen echter ook een belangrijke rol in de bescherming van hun persoonsgegevens. Dropbox geeft je de mogelijkheid om je account te configureren, gebruiken en controleren op een manier die voldoet aan de privacy-, beveiligings- en nalevingseisen van je organisatie. In onze handleiding over gedeelde verantwoordelijkheid lees je meer over wat wij doen om je account veilig te houden en wat jij kunt doen om zichtbaarheid en controle over je persoonsgegevens te handhaven.

# Samenvatting

Elke dag stellen miljoenen gebruikers hun vertrouwen in Dropbox. We willen dat vertrouwen waard zijn, en bouwen Dropbox dus voortdurend verder uit met nadruk op beveiliging en privacy. Ons streven om de persoonsgegevens van onze gebruikers te beschermen, heeft bij al onze beslissingen de hoogste prioriteit. Voor meer informatie kun je contact opnemen via privacy@dropbox.com. Ga voor meer informatie over de GDPR naar ons GDPR-hulpcentrum.