

Privacy en gegevensbescherming

Inleiding

Persoonlijke gegevens spelen een grote rol in de samenleving en de economie. Mensen zijn steeds meer op zoek naar meer controle en duidelijkheid over hoe hun persoonlijke gegevens worden gebruikt en beschermd door de organisaties waarmee ze in contact komen.

Bij Dropbox is vertrouwen de basis van onze relatie met miljoenen mensen en bedrijven over de hele wereld. We waarderen het vertrouwen dat je in ons hebt en nemen de verantwoordelijkheid voor het beschermen van je persoonlijke gegevens serieus.

Onze verplichtingen aan jou

Wij zetten ons in voor het beschermen van je persoonlijke gegevens. In de [servicevoorwaarden](#) van Dropbox worden je verantwoordelijkheden met betrekking tot je gebruik van onze services uiteengezet. In ons [privacybeleid](#) worden onze verplichtingen omtrent privacy van gebruikers beschreven en wordt uitgelegd hoe we je persoonlijke gegevens verzamelen, gebruiken en ermee omgaan wanneer je onze services gebruikt. Als je in Noord-Amerika (Verenigde Staten, Canada en Mexico) woonachtig bent, handelt Dropbox, Inc. als je serviceprovider.

Voor alle andere gebruikers handelt Dropbox International Unlimited Company als beheerder van je persoonlijke gegevens.

Als je een Dropbox Business- of Dropbox Education-gebruiker bent, handelt je organisatie als de gegevensbeheerder voor alle persoonlijke gegevens die aan Dropbox worden geleverd in verband met je gebruik van Dropbox Business of Dropbox Education. De gegevensbeheerder

bepaalt waarom en hoe persoonlijke gegevens worden verwerkt. Dropbox handelt als de gegevensverwerker en verwerkt gegevens namens je organisatie wanneer je Dropbox Business of Dropbox Education gebruikt. In onze [bedrijfsvereenkomst](#) staan verplichtingen omtrent gegevensverwerking en internationale gegevensoverdracht.

Ons trackrecord: naleving

Naleving is een effectieve manier om de betrouwbaarheid van een service te controleren. We moedigen het gebruik van onafhankelijke verificatie aan en leveren deze graag om te laten zien dat onze beveiligings- en privacyprocedures voldoen aan de meest geaccepteerde standaarden en voorschriften, zoals ISO 27001, ISO 27017, ISO 27018, HIPPA/HITECH, Germany BSI C5 en SOC 1, 2 en 3.

Verder waren wij een van de eerste cloudserviceproviders met ISO 27018-certificering, de internationaal erkende standaard voor toonaangevende procedures omtrent cloudprivacy en gegevensbescherming. Onze onafhankelijke externe auditors testen onze controlemechanismen en geven hun eigen rapporten en meningen. Deze kunnen we wanneer mogelijk met je delen.

Hoewel onze certificeringen en auditrapporten over het algemeen gericht zijn op Dropbox Business en Dropbox Education, is de meerderheid van onze controlemechanismen ook van toepassing op Dropbox Basic-, Plus- en Professional-gebruikers. Meer informatie over de standaarden waaraan we voldoen en hoe we onze procedures verifiëren kun je vinden op onze [nalevingswebpagina](#).

Dropbox-architectuur: je persoonlijke gegevens beschermen

Bij Dropbox geloven we dat het beschermen van je persoonlijke gegevens begint bij het veilig houden van je gegevens. Daarom is Dropbox opgebouwd met meerdere beveiligingslagen, zoals veilige gegevensoverdracht, versleuteling en functies op toepassingsniveau, die over een schaalbare, beveiligde infrastructuur zijn verspreid.

Onze infrastructuur: bestanden

De infrastructuur voor bestanden van Dropbox bestaat uit de onderdelen in het onderstaande diagram.



Metadataservers

Bepaalde basisinformatie over gebruikersgegevens, ook wel metagegevens, wordt in een afzonderlijke opslagservice bewaard en fungeert als index voor de gegevens in gebruikersaccounts. Metagegevens omvatten basisinformatie over accounts en gebruikers, zoals e-mailadressen, namen en apparaatnamen. Metagegevens omvatten ook basisinformatie over bestanden, zoals bestandsnamen en -typen, die functies als versiegeschiedenis, herstel en synchronisatie, helpt ondersteunen.

Metagegevensdatabases

Metagegevens over bestanden worden opgeslagen in een MySQL-gebaseerde databaseservice en worden waar nodig gefragmenteerd en gerepliceerd om te voldoen aan de prestatie- en beschikbaarheidsvereisten.

Blokservers

Standaard biedt Dropbox een uniek beveiligingsmechanisme voor de bescherming van gebruikersgegevens dat verder gaat dan traditionele encryptie. Blokservers verwerken bestanden uit de Dropbox-toepassingen door elk bestand op te splitsen in blokken, elk bestandsblok te versleutelen met een sterke encryptie en alleen blokken te synchroniseren die tussen twee 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 encryptie- en toepassingservices op de hoogte van die verandering en worden nieuwe of aangepaste bestandsblokken verwerkt en verzonden naar de opslagserver.

Blokopslagservers

De inhoud van bestanden van gebruikers wordt met de blokopslagservers opgeslagen in versleutelde blokken. Voordat bestanden worden verzonden, worden ze door de Dropbox-client opgesplitst in bestandsblokken ter voorbereiding op de opslag. De blokopslagservers fungeren als een CAS-systeem, wat staat voor Content-Addressable Storage, waarbij elk afzonderlijk versleuteld bestandsblok wordt opgehaald aan de hand van de hashwaarde.

Voorbeeldservers

De voorbeeldservers zijn verantwoordelijk voor het genereren van bestandsvoorbeelden. Voorbeelden zijn een weergave van het bestand van een gebruiker in een andere bestandsindeling die geschikt is voor een snelle weergave op het apparaat van een eindgebruiker. Bestandsblokken worden door voorbeeldservers van de blokopslagservers opgehaald om voorbeelden te genereren. Wanneer een bestandsvoorbeeld wordt aangevraagd, wordt het voorbeeld uit de cache opgehaald van de voorbeeldopslagservers en naar de blokservers overgedragen. Vervolgens worden de voorbeelden door blokservers aan gebruikers getoond.

Voorbeeldopslagservers

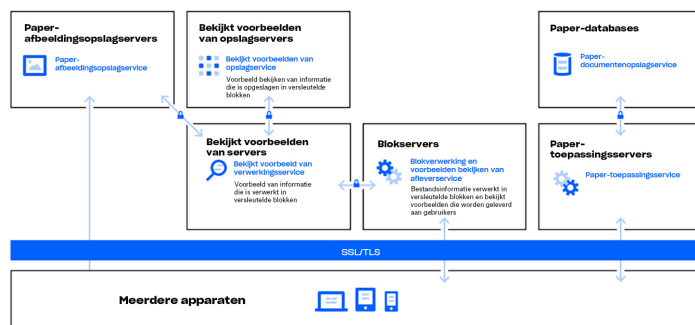
Voorbeelden in cache worden in een versleutelde indeling in de voorbeeldopslagservers opgeslagen.

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(s) 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.

Onze infrastructuur: Paper

Dropbox Paper (Paper) is een functie van het Dropbox-product. Paper gebruikt echter een grotendeels afwijkende set systemen binnen de infrastructuromgeving van Dropbox. De infrastructuur van Paper bestaat uit de onderdelen in het onderstaande diagram.



Paper-appservers

De Paper-appservers verwerken aanvragen van gebruikers, geven de uitvoer van bewerkte Paper-documenten weer aan de gebruiker en voeren meldingsservices uit. Paper-appservers schrijven inkomende bewerkingen van gebruikers naar de Paper-databases, waar ze in permanente opslag worden geplaatst. Communicatiesessies tussen de Paper-appservers en Paper-databases worden versleuteld met een sterke codering.

Paper-databases

De feitelijke inhoud van Paper-documenten van gebruikers, alsmede bepaalde metagegevens over deze Paper-documenten, worden in permanente opslag versleuteld in de Paper-databases. Hiertoe behoort informatie over een Paper-document (bijvoorbeeld titel, gedeeld lidmaatschap, machtigingen en project- en mapkoppelingen), maar ook inhoud uit het Paper-document zelf, waaronder opmerkingen en taken. De Paper-databases worden waar nodig gefragmenteerd en gerepliceerd om te voldoen aan de prestatie- en beschikbaarheidsvereisten.

Opslagervers voor Paper-afbeeldingen

Afbeeldingen die worden geüpload naar Paper-documenten, worden in rust versleuteld opgeslagen op de Paper-afbeeldingservers. De overdracht van afbeeldingsgegevens tussen de Paper-appservers en Paper-afbeeldingservers wordt uitgevoerd via een versleutelde sessie.

Voorbeeldservers

De voorbeeldservers genereren voorbeelden voor zowel afbeeldingen die naar Paper-documenten worden geüpload, als ingesloten hyperlinks in Paper-documenten. Voor afbeeldingen die naar Paper worden geüpload, worden door de voorbeeldservers via een versleuteld kanaal afbeeldingsgegevens opgehaald die in de opslagservers voor Paper-afbeeldingen zijn opgeslagen. Voor hyperlinks die in Paper zijn ingesloten, worden door de voorbeeldservers afbeeldingsgegevens opgehaald en een voorbeeld van de afbeelding gegenereerd via codering, zoals opgegeven door de bronlink. Vervolgens worden de voorbeelden door blokservers aan gebruikers getoond.

Voorbeeldopslagervers

Paper gebruikt dezelfde voorbeeldopslagervers die worden beschreven in het diagram over de Dropbox-infrastructuur om afbeeldingsvoorbeelden in de cache op te slaan. Onderdelen van voorbeelden in cache worden in een versleutelde indeling in de voorbeeldopslagervers opgeslagen.

Controlemechanismen van Dropbox: onze interne procedures

We nemen uitgebreide maatregelen om onze infrastructuur, ons netwerk en onze toepassingen te beschermen. Onze beveiligingsmaatregelen omvatten versleuteling in rust, versleuteling tijdens de overdracht en het permanent verwijderen van bestanden. We bieden ook robuuste privacy- en beveiligingstraining voor al onze werknemers om een cultuur te bouwen waar het onze prioriteit is om je vertrouwen waard te zijn. De details van enkele van onze controlemechanismen worden hieronder beschreven:

Training

Bij het beschermen van de persoonlijke gegevens van onze gebruikers hoort het ontwikkelen en stimuleren van een cultuur van beveiligings- en privacybewustzijn. Dropbox-werknemers gaan verplicht akkoord met beveiligingsbeleidsregels, waaronder een privacybeleid voor gebruikersgegevens, vóór ze toegang krijgen tot de systemen. Werknemers krijgen pas toegang tot dergelijke systemen wanneer ze dit specifiek nodig hebben. Daarnaast nemen werknemers jaarlijks deel aan verplichte beveiligings- en privacytraining.

Encryptie tijdens verzending

Voor een veilige aflevering wordt er een versleutelde verbinding tot stand gebracht om bestandsgegevens tijdens verzending tussen een Dropbox-client (momenteel desktop, mobiel, API of web) en de front-end servers van Dropbox te beschermen. Ook voor de bescherming van Paper-documentgegevens tijdens verzending wordt een versleutelde verbinding tot stand gebracht tussen een Paper-client (momenteel desktop, mobiel, API of web) en de gehoste service. Deze verbindingen worden versleuteld met Secure Sockets Layer (SSL)/Transport Layer Security (TLS) om een beveiligde tunnel te maken die wordt beschermd door 128-bits of hogere AES-versleuteling (Advanced Encryption Standard).

Encryptie in rust

Bestanden die door gebruikers worden geüpload, worden als afzonderlijke bestandsblokken opgeslagen op de opslagserver van Dropbox. Elk blok wordt versleuteld met 256-bits AES-encryptie (Advanced Encryption Standard). Alleen

blokken die tussen twee revisies in zijn aangepast, worden gesynchroniseerd. Ook Paper-documentgegevens die op Paper Databases worden opgeslagen, worden in rust versleuteld met 256-bits AES-encryptie (Advanced Encryption Standard).

Bestanden en Paper-documenten permanent verwijderen

Wanneer een Dropbox-gebruiker of een beheerder van een Dropbox Business- of Dropbox Education-team een bestand selecteert voor permanente verwijdering, wordt hiervoor een proces geactiveerd. Voor het permanent verwijderen van Paper-documentgegevens en afbeeldingsgegevens is er een soortgelijk proces, dat wordt geactiveerd wanneer een gebruiker of de beheerder van een Dropbox Business- of Dropbox Education-team een Paper-document hiervoor selecteert.

Toegangsverzoeken voor persoonlijke gegevens

Als gebruikers toegang willen tot persoonlijke gegevens anders dan de bestanden en Paper-documenten die bij Dropbox zijn opgeslagen, kunnen ze zich aanmelden bij de website en naar hun [accountpagina's](#) gaan. Op de accountpagina wordt informatie opgeslagen zoals de naam die en het e-mailadres dat aan het account is gekoppeld. Gebruikers kunnen ook de IP-adressen van verbonden sessies, computers en mobiele apparaten zien, alsook apps die verbonden zijn met hun accounts, op de [beveiligingspagina](#) en de pagina met [verbonden apps](#).

Dropbox-gebruikers kunnen ook een verzoek indienen voor toegang tot of het verwijderen van persoonlijke gegevens die Dropbox mogelijk over hen heeft verzameld. Meer informatie over dit proces vind je in het [helpcentrum](#) van Dropbox.

Privacybeheer bij Dropbox

Het Privacy Program-team is verantwoordelijk voor het gebruik van het Dropbox Privacy Program. Het implementeert onze belangrijkste privacyinitiatieven en stimuleert ingebouwde privacy in onze levenscyclus van gegevens. Het Dropbox Privacy Program wordt ook ondersteund door verschillende functieoverschrijdende juridische subteams. Deze subteams bieden de extra expertise die nodig is om de dagelijkse taken van het Privacy Program te beheren en te overzien.

Het DPO-team handelt afzonderlijk van de andere privacyfuncties en fungeert als privacy-naleving en toezicht. Het ondersteunt hierbij de functionaris voor gegevensbescherming bij het uitvoeren van diens plichten. De functionaris voor gegevensbescherming (DPO) is de lokale EU-vertegenwoordiger. Je kunt contact opnemen via privacy@dropbox.com.



Grondbeginselen voor informatieverzoeken van de overheid

We begrijpen dat wanneer gebruikers ons hun persoonlijke gegevens toevertrouwen, zij verwachten dat wij vertrouwelijk omgaan met die gegevens. Net als de meeste online diensten krijgen wij soms verzoeken van overheden om informatie over onze gebruikers.

De onderstaande principes beschrijven hoe we omgaan met de informatieverzoeken van overheden die we ontvangen.

Transparant zijn

Het zou online services moeten zijn toegestaan mededelingen te doen over het aantal en het type informatieverzoeken van overheidsinstanties dat ze ontvangen, en mensen te laten weten wanneer informatie over hen wordt opgevraagd. Een dergelijke transparantie geeft gebruikers een beter inzicht in bepaalde verregaande

acties en gedragingen van de overheid. We gaan door met het publiceren van gedetailleerde informatie over deze verzoeken en blijven ons sterk maken voor het recht om meer van deze belangrijke informatie te verstrekken.

Zeer ruim gedefinieerde verzoeken bestrijden

Informatieverzoeken van de overheid moeten worden beperkt tot duidelijk gedefinieerde gegevens en zeer nauwkeurig zijn afgestemd op specifieke mensen en legitieme onderzoeken. We verzetten ons tegen zeer ruim gedefinieerde en bulkverzoeken.

Vertrouwde services aanbieden

Overheden mogen nooit via de achterdeur installaties uitvoeren in online diensten of de infrastructuur ervan aantasten om gebruikersgegevens te verkrijgen. We werken voortdurend aan de beveiliging van onze systemen en blijven ons inzetten voor wetwijzigingen om duidelijk te maken dat dit soort activiteiten illegaal is.

Alle gebruikers beschermen

Bepaalde wetten geven mensen op grond van hun land of nationaliteit verschillende rechten. Dergelijke wetten zijn verouderd en passen niet bij het mondiale karakter van online services. We blijven ons sterk maken voor aanpassing van deze wetten.

Deze principes, alsook ons jaarlijkse transparantierapport, zijn openbaar beschikbaar op de Dropbox-website via:

<https://www.dropbox.com/transparency>.

Zie ons [whitepaper over beveiliging van Dropbox Business](#) (in het Engels) voor meer informatie over onze controlemechanismen en onze aanpak voor het beschermen van je persoonlijke gegevens.

Anderen die voor en met Dropbox werken

De meerderheid van de activiteiten omtrent de inrichting van onze services wordt door Dropbox beheerd. Voor bepaalde services (bijvoorbeeld voor klantensupport en IT-services) maken we echter gebruik van enkele vertrouwde derden. Deze derden krijgen

uitsluitend toegang tot je gegevens om taken uit te voeren namens ons, in overeenstemming met ons [privacybeleid](#). Wij blijven verantwoordelijk voor hun omgang met jouw gegevens conform onze instructies.

Alle derden ondergaan een uitgebreid controleproces, inclusief beveiligingsevaluaties en regelmatige contractuele evaluaties, om te beoordelen of ze kunnen voldoen aan onze verplichtingen inzake gegevensbescherming.

Internationale gegevensoverdrachten

Dropbox is afhankelijk van verschillende juridische mechanismen voor de internationale overdracht van persoonlijke gegevens van de EU naar de Verenigde Staten. We zijn gecertificeerd voor het Amerikaans-Europese Privacy Shield en Amerikaans-Zwitserse Privacy

Shield wat betreft het verzamelen, gebruiken en bewaren van persoonlijke gegevens en hun overdracht van de EU en Zwitserland naar de Verenigde Staten. Naast het Privacy Shield biedt Dropbox ook sterke contractuele garanties

met betrekking tot de privacy van zijn services. Bovendien heeft Dropbox modelcontractclausules van de EU geïmplementeerd om zijn internationale gegevensoverdrachten te dekken.

AVG: de Algemene verordening gegevensbescherming

De Algemene verordening gegevensbescherming (of AVG) is een verordening van de EU die een juridisch kader vaststelt om de persoonlijke gegevens van staatsburgers van EU-lidstaten te beschermen.

De AVG is het belangrijkste onderdeel van de Europese wetgeving inzake gegevensbescherming sinds Databeschermingsrichtlijn van de EU in 1995. Veel bedrijven die zakendoen in Europa, waaronder Dropbox, hebben flink geïnvesteerd in AVG-naleving.

De AVG harmoniseert de wetgeving inzake gegevensbescherming binnen Europa en past deze aan aan de razendsnelle technologische verandering van de afgelopen twintig jaar.

De AVG bouwt voort op eerdere juridische raamwerken in de EU, waaronder de Databeschermingsrichtlijn, en introduceert nieuwe verplichtingen en aansprakelijkheden voor bedrijven die omgaan met persoonlijke gegevens, alsook nieuwe rechten voor individuen wat betreft hun persoonlijke gegevens.

persoonlijke gegevens. Zowel organisaties die in de EU zijn gevestigd als organisaties die de persoonlijke gegevens van staatsburgers van EU-lidstaten verwerken, zijn verplicht om de AVG na te leven.

Het AVG-nalevingstraject van Dropbox

Dropbox zet zich in voor AVG-naleving. Respect voor privacy en beveiliging is vanaf het begin ingebouwd in ons bedrijf. Naarmate we zijn gegroeid, is onze focus op het verwerken en beschermen van de gegevens die onze gebruikers ons toevertrouwen een prioriteit gebleven. Dropbox is een koploper wat betreft naleving en conformiteit. Zoals hierboven al is beschreven, waren wij bijvoorbeeld een van de eerste cloudserviceproviders die ISO 27018-certificering voor hun bedrijfsgebruikers behaalden. In het licht van deze stevige basis beschouwt Dropbox de naleving als een evolutie van onze bestaande praktijken en controlemechanismen, en blijft werken aan initiatieven om ervoor te zorgen dat de persoonlijke gegevens van onze gebruikers altijd worden beschermd.

Meteen toen de AVG in 2016 werd aangenomen, zette Dropbox zich in om de verordening na te leven. De eerste stap was het vormen van een functieoverschrijdend team van gegevensbeschermingsspecialisten, bestaande uit juridisch adviseurs, beveiligings- en nalevingsprofessionals, en product- en infrastructuuringenieurs. Vervolgens voerde ons team een volledige beoordeling van onze huidige beveiligings- en gegevensbeschermingspraktijken uit op basis van de vereisten van de AVG.

De volgende stap was het uitvoeren van een evaluatie van onze verwerkingsactiviteiten van persoonlijke gegevens en het volgen van de levenscyclus van persoonlijke gegevens door onze systemen. Deze oefeningen worden ook wel beschreven als het uitvoeren van gegevenstoewijzingen en het uitvoeren van beoordelingen inzake de impact van gegevensbescherming.

gegevenstoewijzingen en het uitvoeren van beoordelingen inzake de impact van gegevensbescherming.

Sindsdien hebben we voortgebouwd op onze bestaande interne processen en procedures om ervoor te zorgen dat we voldoen aan de rekenschapsprincipes onder de AVG-vereisten. Dit is belangrijk omdat de AVG verhoogde aandacht legt op het documenteren van beslissingen en praktijken die persoonlijke gegevens beïnvloeden.

Onze gebruikers stimuleren op hun reis met AVG

Dropbox biedt functies voor controle en zichtbaarheid waarmee je je verplichtingen inzake gegevensbescherming gemakkelijker kunt beheren, zoals verplichtingen voor AVG-naleving. Natuurlijk komt er veel meer kijken bij de AVG-naleving van je bedrijf dan de relatie met je leveranciers, zoals Dropbox. Onze functies kunnen je helpen je verplichtingen te beheren, maar ze kunnen op zichzelf geen naleving garanderen. AVG-naleving vereist dat je breder denkt over hoe gegevens zich binnen je organisatie bewegen en daar worden beschermd. Elke organisatie moet zelf stappen ondernemen om voor AVG-naleving te zorgen. In dat proces zijn leveranciers belangrijke partners.

Gegevensminimalisatie

Een belangrijk element bij de AVG-vereiste over ingebouwde privacy is dat organisaties hun services moeten ontwikkelen op een manier die gegevens minimaliseert. Dit houdt in dat je een goede zichtbaarheid op en controle over de gegevens binnen je organisatie hebt zodat je deze kunt beheren. Het beheerdersdashboard van Dropbox Business is hierbij een handig hulpmiddel, waarmee je teamactiviteit kunt beheren en verbonden apparaten en activiteiten omtrent het delen van audits kunt bekijken. We werken eraan om de principes van ingebouwde privacy in nieuwe producten en functies in te bouwen.

Bescherming en herstel van gegevens

Bescherming van verloren apparaten, versiegeschiedenis en bestandsherstel kunnen helpen om onbedoeld(e) verlies, schade of vernietiging van persoonlijke gegevens te voorkomen. In geval van een ongeluk kun je hiermee de beschikbaarheid van en toegang tot persoonlijke gegevens tijdig herstellen. Tweestapsverificatie is ook een belangrijke maatregel die we aanraden voor het beschermen van je gegevens.

Records bijhouden

De AVG verhoogt ook de verplichtingen van organisaties om hun verwerkingsactiviteiten nauwkeurig bij te houden. Met onze controlelogboeken en activiteitslogbestanden kun je onze verwerkingsactiviteiten beter begrijpen en zo je eigen administratie ondersteunen.

Toegangsbeheer

Binnen het beheerdersdashboard van Dropbox Business kun je gemakkelijk de toegang van teamleden voor bestanden, mappen en Paper-documenten beheren. Dankzij de functie linkmachtigingen kun je gedeelde bestandslinks beveiligen, vervaldatum instellen om tijdelijke toegang te verlenen en de toegang beperken tot mensen binnen jouw organisatie. Als de verantwoordelijkheden van gebruikers worden gewijzigd, kun je met onze accountoverdrachtstool bestanden en eigendom van Paper-documenten gemakkelijk van de ene gebruiker naar de andere overzetten.

Beheerders kunnen de toegang van een gebruiker tot het eigen account ontzeggen zonder de gegevens en deelactiviteiten aan te tasten, zodat de informatie van je organisatie veilig blijft. Tot slot kun je met de functie voor extern verwijderen

bestanden en Paper-documenten wissen van verloren of gestolen apparaten.

EU-infrastructuur

Hoewel de AVG niet vereist dat persoonlijke gegevens binnen de EU worden gehost, biedt Dropbox gekwalificeerde Dropbox Business- en Dropbox Education-klanten wel de mogelijkheid om bestanden (blokken) in de EU op te slaan. Bestandsopslag in de EU wordt aangeboden via AWS-infrastructuur (Amazon Web Services). Neem voor meer informatie over onze EU-infrastructuur [contact op met ons verkoopteam](#).

Samenwerken om je persoonlijke gegevens te beschermen

Dropbox werkt samen met zijn gebruikers om hun persoonlijke gegevens te beschermen. We nemen de nodige maatregelen om onze infrastructuur, toepassingen en ons netwerk te beschermen, werknemers op te leiden in beveiligings- en privacypraktijken, en een cultuur te bouwen waar de hoogste prioriteit is om andermans vertrouwen waard te zijn.

onderwerpen onze systemen en praktijken aan uitgebreide onafhankelijke tests en controles.

Gebruikers spelen echter ook een belangrijke rol bij het beschermen van hun persoonlijke gegevens. Met Dropbox kun je je account configureren, gebruiken en monitoren op zo'n manier dat je kunt voldoen aan de privacy-,

beveiligings- en nalevingsbehoeften van je organisatie. Onze handleiding over [gedeelde verantwoordelijkheid](#) kan je helpen te begrijpen wat we doen om je account veilig te houden en wat jij kunt doen om de zichtbaarheid op en controle over je persoonlijke gegevens te behouden.

Overzicht

Elke dag vertrouwen miljoen gebruikers op Dropbox. Wij willen dat vertrouwen waard zijn. Daarom hebben we Dropbox ontwikkeld met nadruk op beveiliging en privacy, en blijven we dit doen. Onze toewijding aan het beschermen van de persoonlijke gegevens van onze gebruikers ligt ten grondslag aan elke beslissing die we nemen. Stuur voor meer informatie een e-mail naar privacy@dropbox.com. Voor meer informatie over AVG kun je naar ons [GDPR begeleidingscentrum](#).