Dropbox

Privacy- en gegevensbescherming

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.

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. Als je ingezetene bent van Noord-Amerika (de Verenigde Staten, Canada en Mexico) fungeert Dropbox Inc. als jouw serviceverlener. Voor alle andere gebruikers fungeert Dropbox International Unlimited Company als datacontroller van jouw persoonsgegevens.

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 van en de middelen voor het verwerken van persoonsgegevens.

Dropbox fungeert als dataprocessor en verwerkt gegevens namens jouw organisatie wanneer je Dropbox Business of Dropbox Education gebruikt. In onze overeenkomst voor bedrijven 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 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, ISO 27701, HIPPA/HITECH, 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 functies en geven ons hun rapporten en meningen. We zullen deze waar mogelijk met je delen. Houd er rekening mee dat, hoewel de strekking van onze certificeringen en auditrapporten doorgaans verwijst naar Dropbox Business en Dropbox Education, de meeste van onze controlemechanismen ook van toepassing zijn op gebruikers van Dropbox Basic, Plus en Professional. Bovendien houdt Dropbox zich nu aan de EU Cloud Code of Conduct. Meer informatie over de normen waaraan we voldoen en hoe we onze handelswijzen verifiëren, vind je op onze webpagina over naleving.

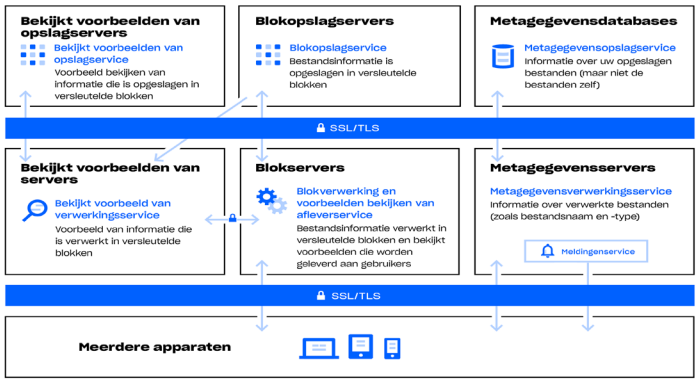
Dropbox

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.



Metagegevensservers

Bepaalde elementaire informatie over gebruikersgegevens die wordt aangeduid als metagegevens, wordt bewaard in een eigen afgezonderde opslagservice en fungeert als een index voor de gegevens in gebruikersaccounts. 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.

Databases met metagegevens

Metagegevens over bestanden 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.

Blokservers

Dropbox biedt 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 Opslagserver.

Blokopslagservers

De daadwerkelijke inhoud van bestanden van gebruikers wordt met deze 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 hash-waarde.

Voorbeeldservers

De voorbeeldservers zijn verantwoordelijk voor het produceren van voorbeelden van bestanden. Voorbeelden geven het bestand van een gebruiker weer in een ander bestandsformaat dat meer geschikt is voor snelle weergave op het apparaat van de eindgebruiker. Voorbeeldservers halen bestandsblokken op uit de blokopslagservers om voorbeelden te genereren. Als er om een bestandsvoorbeeld wordt gevraagd, halen de voorbeeldservers het voorbeeld in de cache van de voorbeeldopslagservers op en sturen het naar de blokservers. Voorbeelden worden uiteindelijk door blokservers aan gebruikers getoond.

Voorbeeldopslagservers

Voorbeelden in de cache worden in een versleuteld formaat opgeslagen in de voorbeeldopslagservers.

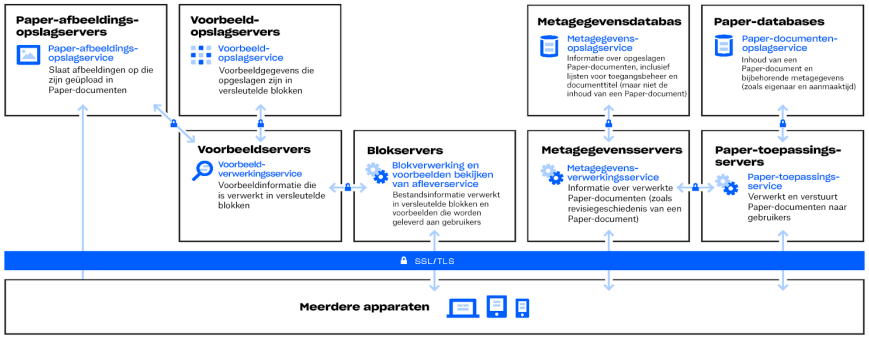
Meldingsservice

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.

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-databases

De daadwerkelijke inhoud van Paper-documenten van gebruikers, evenals bepaalde metagegevens van deze Paper-documenten, wordt 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-afbeeldingsopslagservers

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

Voorbeeldservers

De voorbeeldservers produceren voorbeelden van afbeeldingen die naar Paper-documenten zijn geüpload en van hyperlinks die in Paper-documenten zijn ingesloten. Voor afbeeldingen die naar Paper-documenten zijn geüpload, halen de voorbeeldservers via een gecodeerd kanaal afbeeldingsgegevens op die zijn opgeslagen in de opslagservers voor Paper-afbeeldingen. Voor hyperlinks die in Paper-documenten zijn ingesloten, halen voorbeeldservers de afbeeldingsgegevens op en geven een voorbeeld van de afbeelding weer met behulp van versleuteling zoals gespecificeerd door de bronlink. Voorbeelden worden uiteindelijk door blokservers aan gebruikers getoond.

Voorbeeldopslagservers

Paper gebruikt dezelfde voorbeeldopslagservers als beschreven in het Dropbox-infrastructuurdiagram voor het opslaan van voorbeelden van afbeeldingen in de cache. Delen van voorbeelden in de cache worden versleuteld opgeslagen in de voorbeeldopslagservers.

Dropbox

Controlemechanismen van Dropbox: interne procedures

We nemen uitvoerige maatregelen om onze infrastructuur, ons netwerk en onze toepassingen te beschermen. Enkele beveiligingsmaatregelen die we hebben getroffen, zijn versleuteling tijdens inactiviteit, versleuteling tijdens verzending en het definitief verwijderen van bestanden. Ook bieden wij al onze werknemers een gedegen privacy- en beveiligingstraining om 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 beveiligingsbeleid, waaronder een privacybeleid voor gebruikersgegevens, om toegang tot systemen te krijgen. Alleen die werknemers die voor een specifiek doel toegang moeten hebben, hebben toegang tot dergelijke systemen. Werknemers nemen ook ieder jaar deel aan verplichte beveiligings- en privacytrainingen.

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 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-documentengegevens 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 tot persoonsgegevens

Om naast de bestanden en Paper-documenten die in Dropbox zijn opgeslagen ook toegang te verkrijgen tot persoonsgegevens, 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 Dropbox mogelijk over hen heeft verzameld. Ga voor meer informatie over dit proces naar het Helpcentrum van Dropbox.

Privacybeheer bij Dropbox

Het Privacy team is verantwoordelijk voor de uitvoering van het Dropbox Privacy-programma. Dit team voert onze belangrijkste initiatieven op het gebied van privacy uit en staat garant voor de privacy in de levenscyclus van onze gegevens. Het Dropbox Privacy-programma wordt ook ondersteund door meerdere multidisciplinaire juridische subteams. Deze subteams beschikken over de aanvullende expertise die noodzakelijk is om toezicht te houden op de dagelijkse taken van het privacyprogramma.

Het DPO-team werkt apart van de andere privacy-afdelingen en biedt rechtstreeks ondersteuning en overzicht aan de verantwoordelijke voor gegevensbescherming (Data Protection Officer) op het gebied van naleving van privacy, zodat die zijn werkzaamheden kan uitvoeren. Je kunt contact opnemen met de Data Protection Officer (DPO) via privacy@dropbox.com.

Dropbox

Grondbeginselen voor gegevensverzoeken van de overheid

Wanneer gebruikers ons hun persoonsgegevens toevertrouwen, verwachten zij van ons dat wij deze vertrouwelijk houden. Net zoals de meeste online services 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 deze belangrijke informatie te verstrekken.

Strijden tegen 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 services 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/transparency.

Voor meer informatie over onze functies en onze kijk op de bescherming van je persoonsgegevens, kun je de whitepaper over beveiliging van Dropbox Business raadplegen.

Anderen die voor en met 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, en we blijven verantwoordelijk voor hun verwerking van jouw gegevens conform onze instructies.

Iedere derde wordt streng gecontroleerd, onder andere op beveiliging en privacy, en ook wordt regelmatig nagegaan of de derde aan de contractuele verplichten voldoet. Zo kunnen wij beoordelen of de partij in kwestie in staat is om te voldoen aan onze beloften op het gebied van gegevensbescherming. Op basis van deze controle bevestigt Dropbox dat de vertrouwde derden zich inzetten om te voldoen aan de geldende EU-wetgeving op het gebied van gegevensbescherming wanneer zij namens Dropbox persoonlijke gegevens verwerken.

Klanten kunnen de vertrouwde derde partijen van Dropbox controleren door inzage in de ISO 27001- en 27018-certificeringen van Dropbox en, overeenkomstig de relevante geheimhoudingsplicht, in het SOC 2 Type II-rapport van Dropbox. Bovendien kunnen klanten de door Dropbox vertrouwde derden controleren door de beheersingsmaatregelen en auditresultaten voor Trust Services Criteria P6.1, P6.4 en CC.9.2 uit het SOC 2 Type II-rapport te lezen.

Dropbox

Internationale gegevensoverdracht

Wanneer er gegevens worden overgedragen vanuit de Europese Unie, de Europese Economische Ruimte, het Verenigd Koninkrijk en Zwitserland, hanteert Dropbox diverse juridische mechanismen, zoals contracten met onze klanten en gelieerde ondernemingen, standaard contractbepalingen en adequaatheidsbesluiten van de Europese Commissie over bepaalde landen, voor zover van toepassing.

Dropbox voldoet aan de Amerikaans-Europese en Amerikaans-Zwitserse Data Privacy Frameworks, evenals de Britse uitbreiding van het Amerikaans-Europese Data Privacy Framework zoals omschreven door het Amerikaanse Department of Commerce inzake het verwerken van persoonlijke gegevens die van de Europese Unie, de Europese Economische Ruimte, het Verenigd Koninkrijk en Zwitserland worden overgebracht naar de Verenigde Staten. Dropbox heeft een certificeringsverklaring ingediend bij het Amerikaanse Department of Commerce waarin wordt aangegeven dat Dropbox zich met betrekking tot dergelijke gegevens aan deze beginselen van de Privacy Frameworks houdt. Het DocSend- of Formshifts-gedeelte van de Services is hier echter niet bij inbegrepen.

Voor meer informatie over het Data Privacy Framework, en om de certificering van Dropbox te bekijken, ga je naar www.dataprivacyframework.gov.

Klachten en geschillen met betrekking tot onze naleving van de Data Privacy Framework-principes worden onderzocht en opgelost door JAMS, een onafhankelijke externe partij. Meer informatie kun je vinden in ons Privacybeleid.

AVG: de Algemene verordening gegevensbescherming

De AVG, ook wel de Algemene verordening gegevensbescherming of AVG genoemd, is een EU-verordening die een juridisch kader vaststelt ter bescherming van de persoonsgegevens van betrokkenen uit de EU. De AVG 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 AVG stemt wetgeving uit heel Europa op het gebied van gegevensbescherming op elkaar af en maakt deze geschikt 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 gevestigd zijn in de EU en organisaties die persoonsgegevens van gegevensonderwerpen uit de EU verwerken, moeten verplicht voldoen aan de AVG.

Het AVG-nalevingsproces van Dropbox

Dropbox streeft naar volledige naleving van de AVG. Al vanaf het begin vormen privacy en beveiliging de hoeksteen van ons bedrijf, en hoezeer 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 AVG als logische volgende stap voor onze bestaande praktijken en functies en hanteert het bedrijf een doorlopende, voortdurend in ontwikkeling zijnde set initiatieven die waarborgen dat de persoonsgegevens van gebruikers altijd worden beschermd. Het proces van Dropbox voor naleving van de AVG 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 AVG-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 AVG-vereisten, zoals het bijhouden van een register van de verwerkingsactiviteiten overeenkomstig artikel 30 van de AVG. Dit is van belang omdat de AVG sterk is gericht op het documenteren van beslissingen en praktijken die invloed op persoonsgegevens hebben.

Dropbox

Onze gebruikers helpen bij hun AVG-processen

Dropbox biedt controle- en zichtbaarheidsfuncties waarmee je gemakkelijker je verplichtingen omtrent gegevensbescherming kunt beheren, waaronder AVG-nalevingseisen. Natuurlijk staat of valt AVG-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 AVG-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 AVG-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 zijn en goed kunnen worden gecontroleerd, zodat je ze eenvoudig kunt beheren. Het Dropbox Business-beheerdashboard is hiervoor een handig hulpprogramma, omdat je hiermee je teamactiviteit kunt bijhouden, verbonden apparaten kunt weergeven en deelactiviteiten kunt beoordelen. We zijn bezig om de Privacy by Design-principes te verweven in nieuwe producten en functies.

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 AVG 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 Business-beheerdashboard kun je de toegang voor teamleden tot bestanden, mappen en Paper-documenten eenvoudig 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 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 gebruiker de toegang 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

Het is voor de AVG 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 binnen de EU wordt aangeboden via de AWS-infrastructuur (Amazon Web Services). Voor meer informatie over onze EU-infrastructuur kun je contact opnemen met ons verkoopteam.

Samenwerken aan de bescherming van je persoonsgegevens

Dropbox werkt samen met 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 onderwerpen onze systemen en werkwijzen aan strenge testen en audits voor derden.

Maar gebruikers vervullen een sleutelrol bij het beschermen van hun persoonlijke gegevens. Op Dropbox kun je je account zodanig configureren, gebruiken en controleren dat er wordt voldaan aan de behoeften van jouw bedrijf op het gebied van privacy, beveiliging en naleving. Via onze gids met gezamenlijke verantwoordelijkheden krijg je meer inzicht in wat wij doen om je account veilig te houden en wat jij kunt doen om zicht op, en controle over, jouw persoonlijke gegevens te houden.

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 AVG naar ons AVG-hulpcentrum.