



Apple in het onderwijs

Overzicht voor scholen

over de privacy van gegevens

Inhoud

[Wat Apple doet om de privacy van leerlingen te beschermen](#)
[Apple School Manager en beheerde Apple ID's](#)
[Schoolwerk](#)
[Klaslokaal](#)
[Beheerde Apple ID's en Gedeelde iPad](#)
[iCloud en gegevensbeveiliging](#)
[CloudKit en apps van andere ontwikkelaars](#)
[Locatievoorzieningen en Verloren-modus](#)
[Analytische informatie](#)
[Internationale gegevensoverdracht](#)
[Privacyoverzicht voor ouders](#)
[Aanvullende informatiebronnen](#)

De technologie van Apple speelt alweer 40 jaar een belangrijke ondersteunende rol in het onderwijs. Onze veelzijdige tools en apps maken het leerproces aantrekkelijker en stimuleren de creativiteit van iedere leerling. We weten hoe belangrijk beveiliging en privacy zijn, en dat alle gegevens die leerlingen al doende aanmaken, bewaren en raadplegen, goed moeten worden afgeschermd.

Beveiliging en privacy zijn fundamentele elementen in het ontwerp van alle hardware, software en voorzieningen van Apple. We pakken dit op een geïntegreerde manier aan, om de beveiliging en privacy zo goed mogelijk te waarborgen. Die aanpak is berekend op alle soorten gebruikers, ook binnen een onderwijssetting, zoals leerkrachten, andere medewerkers op een school en leerlingen.

Daarnaast hebben we speciale functies en voorzieningen voor het onderwijs ontwikkeld, namelijk Apple School Manager, beheerde Apple ID's en Gedeelde iPad. Bij het ontwerp hebben we dezelfde geïntegreerde aanpak gebruikt, met extra aandacht voor de specifieke beveiligings- en privacyeisen in het onderwijs.

In dit overzicht wordt uitgelegd hoe beheerde Apple ID's en de bijbehorende onderwijsfuncties en -voorzieningen omgaan met de gegevens van leerlingen en hun privacy. U kunt uit dit overzicht putten als u ouders wilt informeren over hoe Apple de gegevens van hun kind afschermt.

Let op: Sommige voorzieningen, apps en boeken zijn niet in alle landen beschikbaar. Controleer welke er in uw land beschikbaar zijn.

Wat Apple doet om de privacy van leerlingen te beschermen

Apple zal nooit gegevens van leerlingen bijhouden, delen of verkopen voor reclame- of marketingdoeleinden. We stellen geen profielen op van leerlingen op basis van hun e-mails of surfgedrag. Voor zover we persoonlijke gegevens van leerlingen verzamelen, gebruiken of vrijgeven, doen we dat alleen binnen het kader van onze onderwijsservices. Apple zal nooit persoonlijke gegevens van leerlingen verkopen of vrijgeven voor gerichte reclamedoeleinden.

In het [Apple privacybeleid](#) plus de [Apple School Manager-overeenkomst](#) is vastgelegd hoe we gegevens van gebruikers verzamelen, gebruiken, vrijgeven, overdragen en bewaren. Verder hebben we de [Student Privacy Pledge](#) ondertekend.

Apple School Manager en beheerde Apple ID's

Apple reikt scholen en instellingen in alle soorten en maten voorzieningen aan om de implementatie van iPad en Mac te vergemakkelijken. Al bij de ontwikkeling van deze voorzieningen is rekening gehouden met beveiliging en privacy. Hierdoor zijn de gegevens van uw instelling en van de leerlingen voor, tijdens en na de implementatie goed afgeschermd.

Apple School Manager is een gratis webvoorziening waarmee IT-beheerders alles kunnen regelen voor de implementatie van iPad en Mac op school. In Apple School Manager kunt u content kopen, de automatische aanmelding in uw MDM-oplossing (Mobile Device Management) configureren, accounts aanmaken voor uw leerlingen en andere gebruikers, lesroosters instellen voor de Schoolwerk- en Klaslokaal-app, de voortgang bijhouden in Schoolwerk en apps en boeken beheren voor zowel leerkrachten als leerlingen.

Een belangrijke functie van Apple School Manager is het aanmaken van beheerde Apple ID's. Beheerde Apple ID's geven leerlingen toegang tot iCloud Drive, iCloud-fotobibliotheek, iCloud-reservekopie, Schoolwerk en Gedeelde iPad, terwijl u als school toch de touwtjes in handen houdt. Beheerde Apple ID's zijn specifiek voor het onderwijs bedoeld.

Om ervoor te zorgen dat leerlingen de devices die hun school ter beschikking stelt alleen gebruiken voor hun schoolwerk, hebben we bepaalde functies van beheerde Apple ID-accounts uitgeschakeld. Zo kunnen leerlingen geen aankopen doen in de App Store, iBooks Store of iTunes Store. Verder zijn Apple Pay, Zoek mijn vrienden, Zoek mijn iPhone, iCloud-mail, HomeKit en iCloud-sleutelhanger uitgeschakeld. FaceTime en iMessage staan ook standaard uit, maar kunnen door een beheerder worden ingeschakeld.

In Apple School Manager kunt u beheerde Apple ID's automatisch laten genereren voor alle leerlingen en leerkrachten. U importeert dan alleen de benodigde gegevens vanuit het schoolinformatiesysteem (SIS) of vanuit csv-bestanden die uit adressenlijsten zijn geëxporteerd. Elke gebruikersaccount wordt aangemaakt met niet-bewerkbare gegevens uit het bronbestand. Aanvullende informatie, zoals de identificatiecode van de beheerde Apple ID en het bijbehorende wachtwoord, wordt in Apple School Manager toegevoegd aan de accountgegevens. Er worden in geen geval gegevens naar het SIS geschreven.

Aan elke gebruikersaccount kan de onderstaande informatie gekoppeld zijn, die te zien is in de accountlijst of bij het selecteren van een specifieke account:

- Een unieke alfanumerieke code
- Voornaam, tweede naam en achternaam
- Klas of groep (indien ingevoerd)
- Aangemelde klassen
- E-mailadres (indien ingevoerd)
- Rol
- Locatie
- Bron
- Datum aangemaakt
- Datum gewijzigd

De school maakt deze beheerde Apple ID's zelf aan en wijst ze ook zelf toe. Daarom is het heel eenvoudig om wachtwoorden te resetten, accounts te inspecteren en rollen te definiëren. Zodra een beheerder een account inspecteert of een wachtwoord wordt gereset, wordt dit automatisch vastgelegd in een logboek. Zo kunt u altijd nagaan wat er precies is gebeurd.

Beheerde Apple ID's ondersteunen allerlei soorten toegangscode, van eenvoudige codes van vier cijfers tot complexe alfanumerieke combinaties. Apple School Manager stelt een tijdelijk wachtwoord in voor nieuw aangemaakte of geïmporteerde accounts. Daarmee kunnen gebruikers voor de eerste keer inloggen, waarna ze meteen een ander wachtwoord moeten instellen. Zodra een leerling dit heeft gedaan, laat Apple School Manager nooit het nieuwe wachtwoord zien. Leerlingen kunnen ook bij hun bestanden van school op een device dat niet door de instelling wordt beheerd, bijvoorbeeld op een device thuis. Ze loggen dan in met hun beheerde Apple ID, wachtwoord en een verificatiecode van zes cijfers die de beheerder via Apple School Manager heeft toegewezen. Deze verificatiecode verloopt automatisch na één jaar.

Wanneer een instelling een beheerde Apple ID verwijdert, wordt alle aan die account gekoppelde informatie binnen maximaal 30 dagen van de Apple servers verwijderd. En wanneer een school besluit te stoppen met het gebruik van Apple School Manager, worden alle gegevens over leerlingen binnen maximaal 180 dagen verwijderd.

Schoolwerk

Met de Schoolwerk-app kunnen leerkrachten instructiemateriaal delen en meer inzicht krijgen in de voortgang van leerlingen via de apps en boeken die ze voor hen gebruiken. Schoolwerk maakt gebruik van informatie over leerlingen en lesroosters die beheerders in Apple School Manager hebben ingevoerd. Desgewenst kan een school in Apple School Manager instellen dat de voortgang van leerlingen mag worden bijgehouden in de Schoolwerk-app. Dan kunnen app-ontwikkelaars ervoor zorgen dat de voortgang van leerlingen afgeschermd en veilig wordt gedeeld met hun leerkrachten. Het gaat dan om activiteiten die in een door de school beheerde omgeving worden toegewezen, zoals het lezen van een hoofdstuk in een studieboek, het maken van wiskundesommen of het afleggen van een toets. Zo krijgen leerkrachten én leerlingen meer inzicht in hoe het gaat met alle lesopdrachten. Waar nodig kunnen leerkrachten voor extra opdrachten of begeleiding zorgen.

Wanneer lesactiviteiten via de Schoolwerk-app worden opgegeven, krijgt de leerkracht inzicht in de voortgangsgegevens die door de deelnemende app wordt gegenereerd. Denk bijvoorbeeld aan:

- Bestede tijd
- Begin- en eindtimers
- Score bij toetsen
- Geboekte vooruitgang
- Verdiende punten
- Een binaire waarde als Ja/Nee, Waar/Onwaar, Volledig/Onvolledig

De bescherming van de privacy van leerlingen zit in het ontwerp van Schoolwerk geworteld. Wanneer een school in Apple School Manager heeft ingesteld dat de voortgang van leerlingen mag worden bijgehouden in Schoolwerk, worden de desbetreffende gegevens alleen gedeeld voor activiteiten die de leerkracht specifiek als opdracht heeft toegewezen in de Schoolwerk-app, en dan alleen nog wanneer leerlingen op hun device de beheerde Apple ID gebruiken die hun school voor ze heeft gemaakt. De voortgang van leerlingen bij activiteiten die niet specifiek op deze manier zijn toegewezen, worden niet gedeeld of weergegeven. Stel, een leerkracht wijst leerlingen de opdracht toe om de proloog van *Romeo en Julia* te lezen in iBooks. Een van de leerlingen leest daarnaast ook *The Great Gatsby*. Leerling en leerkracht krijgen in dit geval alleen de voortgangsgegevens te zien over de proloog, omdat dat de toegewezen leesopdracht was. Met het oog op de transparantie krijgen leerlingen een melding om ze erop te wijzen dat hun voortgang wordt vastgelegd (wanneer de school dat heeft ingeschakeld).

Klaslokaal

Met de Klaslokaal-app kunnen leerkrachten de iPads van de leerlingen in hun klas beheren en hun leerlingen in de les begeleiden door apps en koppelingen voor ze te openen. Leerkrachten kunnen eenvoudig documenten uitwisselen met iedereen in de klas en het werk van leerlingen in de gaten houden door op hun scherm mee te kijken.

Met Klaslokaal kunnen de iPad-devices van leerlingen alleen tijdens de les worden beheerd. Na afloop worden er geen gegevens bewaard. De leerkracht en leerlingen moeten bij elkaar in de buurt zitten en aangemeld zijn bij hetzelfde wifinetwerk. Bovendien moet er een klassensessie geactiveerd zijn. Buiten de les kan de leerkracht devices van leerlingen niet beheren of bekijken. Als Schermweergave actief is voor het scherm van een leerling in de klas, verschijnt hierover een melding boven in het scherm van de leerling. Die weet dus altijd wanneer de leerkracht op zijn scherm meekijkt. Scholen kunnen Schermweergave ook uitschakelen als ze niet willen dat leerkrachten het scherm van leerlingen kunnen bekijken.

Beheerde Apple ID's en Gedeelde iPad

Als leerlingen een iPad met elkaar moeten delen, loggen ze in met een beheerde Apple ID. Zo kunnen ze altijd werken met hun eigen apps, content en instellingen. Op deze manier kunnen meerdere leerlingen dezelfde iPad gebruiken, want ze werken allemaal in hun eigen gedeelte.

Zodra een leerling inlogt bij Gedeelde iPad, wordt de beheerde Apple ID automatisch geverifieerd met de identiteitsservers van Apple. Als de leerling dat device voor het eerst gebruikt, worden automatisch een nieuwe thuismap en sleutelhanger voor die gebruiker aangemaakt. Zodra de lokale account van de leerling is aangemaakt en ontgrendeld, wordt het device automatisch aangemeld bij iCloud. Vervolgens worden de instellingen van de leerling bewaard en worden documenten en gegevens gesynchroniseerd vanuit iCloud.

Zolang een sessie actief is en het device online blijft, worden alle documenten en gegevens bewaard in iCloud zodra ze worden aangemaakt of gewijzigd. Op de achtergrond loopt nog een synchronisatieproces dat ervoor zorgt dat alle wijzigingen in iCloud worden bewaard wanneer de leerling uitlogt.

iCloud en gegevensbeveiliging

Terwijl de leerlingen nieuwe documenten aanmaken, interactief met hun lessen werken en meedoen aan klassikale activiteiten, is het belangrijk dat ze alles veilig en goed afgeschermd kunnen bewaren, zowel op het device zelf als in iCloud.

Dankzij iCloud worden al hun documenten, contactgegevens, notities, bladwijzers, agenda's en herinneringen automatisch bewaard. Bovendien hebben ze er altijd toegang toe op hun iOS-device en Mac, plus via [iCloud.com](https://www.icloud.com) op een Mac of pc. Voor beheerde Apple ID's zijn de bovenstaande voorzieningen standaard ingeschakeld en gebruikers krijgen 200 GB gratis opslagruimte in iCloud. Zodra een gebruiker zich aanmeldt bij iCloud, krijgen apps toegang tot iCloud Drive. De gebruiker kan deze toegang per app instellen onder 'Instellingen' > 'iCloud'.

iCloud is ontwikkeld volgens gangbare beveiligingsnormen en werkt met strenge gegevensbeveiligingsprotocollen. iCloud beveiligt gebruikersgegevens door deze te coderen voordat ze via het internet worden verzonden, door ze gecodeerd te bewaren op de server en door veilige tokens te gebruiken voor identiteitscontrole. Dit betekent dat de gegevens van leerlingen beschermd zijn tegen ongeoorloofde toegang wanneer ze naar een device worden verzonden en wanneer ze in iCloud worden bewaard. iCloud maakt gebruik van minimaal 128-bits AES-versleuteling, dezelfde beveiliging die in gebruik is bij grote financiële instellingen. Coderingssleutels worden in de datacenters van Apple bewaard en worden nooit doorgegeven aan derden. iCloud bewaart verder de wachtwoorden en verificatiegegevens van leerlingen op zo'n manier dat Apple ze niet kan lezen en er geen toegang toe heeft.

Apple is gecertificeerd volgens ISO 27001 en ISO 27018 voor het implementeren van een Information Security Management System (ISMS) met maatregelen ter bescherming van persoonsgegevens in openbare cloudomgevingen. Certificering voor naleving van de ISO-norm is aan Apple verleend door de British Standards Institution (BSI). Op de website van de BSI vindt u de compliance-certificaten voor [ISO 27001](#) en [ISO 27018](#).

Op de webpagina [Overzicht van iCloud-beveiliging](#) staat nog meer informatie.

CloudKit en apps van andere ontwikkelaars

Apps van andere ontwikkelaars zijn onontbeerlijk in een moderne leeromgeving. We willen dat leerlingen ook in die apps naadloos hun gegevens kunnen bewaren en ophalen. Daarom hebben we CloudKit gemaakt, een framework dat andere ontwikkelaars kunnen gebruiken om gegevens te bewaren en te synchroniseren naar iCloud.

In een app die CloudKit gebruikt, worden leerlingen automatisch aangemeld met hun beheerde Apple ID. Ze hoeven dus geen nieuwe account aan te maken of andere persoonlijke informatie in te voeren. Zo hebben ze altijd toegang tot de meest actuele informatie in de app zonder dat ze een andere gebruikersnaam of een ander wachtwoord hoeven te onthouden. Ontwikkelaars hebben geen toegang tot de beheerde Apple ID van leerlingen, alleen tot een unieke identificatiecode.

Ongeacht het feit of een ontwikkelaar CloudKit wel of niet gebruikt, het is altijd mogelijk dat apps van andere ontwikkelaars gegevens over leerlingen verzamelen. Het is de taak van de school om erop toe te zien dat alle relevante wet- en regelgeving wordt nageleefd bij het gebruik van apps van andere ontwikkelaars.

De school moet zich goed verdiepen in de voorwaarden, beleidsteksten en werking van dit soort apps, en dan met name nagaan of er gegevens van leerlingen worden verzameld, wat daarmee wordt gedaan en of de toestemming van ouders vereist is.

Ontwikkelaars die hun app via onze App Store willen distribueren, moeten akkoord gaan met specifieke richtlijnen die zijn opgesteld om de privacy en veiligheid van de gebruiker te garanderen. We stellen aanvullende eisen aan alle ontwikkelaars die met ons ClassKit-framework apps gaan ontwikkelen voor het bijhouden van de voortgang van leerlingen in Schoolwerk. Naast onze standaardvereisten voor de publicatie van apps in de App Store geldt voor ClassKit dat ontwikkelaars dit framework alleen mogen gebruiken voor het ontwikkelen van diensten op het gebied van onderwijs. Ze mogen niet gericht adverteren in de app en moeten in een passend privacybeleid vastleggen waarvoor ze alle gegevens gebruiken.

Als we ontdekken dat een app deze richtlijnen schendt, moet de ontwikkelaar het probleem oplossen. Als dat niet gebeurt, wordt de app uit de App Store verwijderd.

Locatievoorzieningen en Verloren-modus

Bij het gebruik van de apps en voorzieningen op hun device krijgen leerlingen mogelijk de vraag voorgeschoteld of ze locatievoorzieningen willen inschakelen. Apple geeft gebruikers de optie om heel gericht in te stellen wat er met locatiegegevens gebeurt en in hoeverre die worden gedeeld met apps en cloudvoorzieningen. Locatievoorzieningen zijn standaard uitgeschakeld, maar kunnen door de leerlingen worden ingeschakeld als de school dat toestaat.

De ingebouwde locatiegerichte apps van Apple (zoals Kaarten, Weer of Camera) hebben toestemming van de gebruiker nodig om locatiegegevens te kunnen verzamelen en gebruiken. Uit de locatiegegevens die Apple verzamelt, is niet te herleiden van welke specifieke leerling ze afkomstig zijn. Ook andere door de school beschikbaar gestelde apps moeten de gebruiker toestemming vragen om toegang te krijgen tot locatiegegevens. Net als al onze klanten kunnen leerlingen per app aangeven of die wel/geen gebruik mag maken van locatiegegevens en die toestemming altijd weer intrekken.

Ze kunnen dan kiezen om het nooit toe te staan, alleen bij gebruik of altijd, afhankelijk van de app. Gebruikers kunnen die toegang ook weigeren en hun keuze altijd in 'Instellingen' aanpassen. Bovendien krijgt de gebruiker een melding als een app locatiegegevens op de achtergrond gebruikt, ook als hij daar toestemming voor heeft gegeven. De gebruiker kan zijn keuze dan alsnog aanpassen. Als een app gebruikmaakt van Locatievoorzieningen, is in de menubalk het symbool van een pijl te zien.

De locatie van een gebruiker is via de functies en voorzieningen van Apple niet automatisch beschikbaar voor de school. Locatievoorzieningen kunnen echter wel worden ingezet om een school te helpen een zoekgeraakt of gestolen device te vinden. Op een schooldevice kan een MDM-beheerder op afstand de Verloren-modus inschakelen. De gebruiker wordt dan uitgelogd en het device kan niet meer worden ontgrendeld. Op het scherm wordt een melding weergegeven die door de beheerder kan worden aangepast. Denk bijvoorbeeld aan het verzoek om een bepaald telefoonnummer te bellen wanneer iemand het device vindt. De beheerder kan een device in de Verloren-modus een verzoek sturen om de huidige locatie door te geven aan de MDM-server. Wanneer een beheerder de Verloren-modus uitschakelt, wordt de locatie van het device verzonden en wordt dat gemeld aan de gebruiker.

Analytische informatie

Als u en uw leerlingen ons willen helpen de producten en diensten van Apple te verbeteren, kunt u zich aanmelden bij ons Analytics Program. Er wordt dan anonieme informatie over devices en apps naar Apple gestuurd.

Hiervoor moet u expliciet toestemming geven. Gebruikers kunnen deze gegevens inzien op hun device of het verzenden daarvan altijd stopzetten in 'Instellingen'. Als uw school gebruikmaakt van gedeelde iPads, kan het versturen van analytische gegevens via een beperking worden uitgeschakeld.

iOS bevat ook geavanceerde diagnostische voorzieningen die nuttig kunnen zijn bij het opsporen van fouten of het oplossen van problemen met devices. Deze voorzieningen versturen geen gegevens naar Apple zonder aanvullende hulpprogramma's en uitdrukkelijke goedkeuring.

Internationale gegevensoverdracht

Apple werkt met scholen over de hele wereld om leerkrachten en klaslokalen te voorzien van de beste onderwijsstools. Daarnaast werken we samen met bestuursorganen om er zeker van te zijn dat onze diensten voldoen aan alle vereisten voor gegevensverwerking.

Bij het gebruik van Apple School Manager, beheerde Apple ID's, en iCloud kan het voorkomen dat persoonlijke gegevens ergens buiten het land van oorsprong worden opgeslagen. Dat maakt op zich niet uit, want overal gelden dezelfde strenge normen en eisen voor gegevensopslag.

Apple waarborgt dat persoonlijke gegevens die vanuit de Europese Economische Ruimte of Zwitserland naar de VS worden verzonden, onderworpen zijn aan door de Europese Commissie goedgekeurde modelcontracten voor de EER of aan een Swiss Transborder Data Flow Agreement voor Zwitserland, of aan enig certificeringsprogramma ter bescherming van de privacy dat van kracht is en waarvoor Apple Inc. mogelijk gecertificeerd wordt. De modelcontracten en de Swiss Transborder Data Flow Agreement zijn als bijlage toegevoegd aan de Apple School Manager-overeenkomst.

Privacyoverzicht voor ouders

Transparantie is van groot belang om inzicht te kunnen bieden in de manieren waarop informatie van leerlingen wordt gebruikt. Om vragen van ouders of verzorgers te beantwoorden, hebben we een [privacyoverzicht voor ouders](#) gemaakt. We raden u aan dit overzicht te verspreiden onder alle belanghebbenden op uw school. Hierin wordt uitgebreid uitgelegd hoe informatie van leerlingen wordt verzameld, wat ermee wordt gedaan en hoe deze wordt bewaard wanneer scholen onderwijsdiensten en apps van Apple gebruiken.

Aanvullende informatiebronnen

Voor Apple is het van cruciaal belang dat uw school en leerlingen op ons kunnen vertrouwen. Daarom respecteren we de privacy van leerlingen en beschermen we die met geavanceerde versleutelingstechnieken en een strikt beleid waarin is vastgelegd hoe er met alle gegevens wordt omgegaan.

Lees de informatiebronnen hieronder als u nog meer wilt weten. Hebt u specifieke vragen over privacy? Dan kunt u ons rechtstreeks benaderen via www.apple.com/benl/privacy/contact.

- Over privacy en beveiliging van Apple producten in het onderwijs:
<https://support.apple.com/kb/HT208525>
- Privacyoverzicht voor ouders:
https://images.apple.com/education/docs/Privacy_Overview_for_Parents.pdf
- Apple en het onderwijs, IT en implementatie:
<https://www.apple.com/nl/education/it/>
- Apple School Manager-overeenkomst:
<https://www.apple.com/legal/education/apple-school-manager/>
- Apple School Manager Help:
<https://help.apple.com/schoolmanager/>
- Implementatiehandleiding voor het onderwijs:
<https://help.apple.com/deployment/education/>
- Handleiding 'iOS-beveiliging':
https://www.apple.com/nl/business/docs/iOS_Security_Guide.pdf
- Wat Apple doet om uw privacy te beschermen:
<https://www.apple.com/benl/privacy/>



© 2018 Apple Inc. Alle rechten voorbehouden. Apple, het Apple logo, Apple Pay, FaceTime, iMessage, iPad, iPhone, iTunes U en Mac zijn handelsmerken van Apple Inc., die zijn gedeponeerd in de Verenigde Staten en andere landen. HomeKit is een handelsmerk van Apple Inc. App Store, CloudKit, iBooks Store, iCloud, iCloud Drive, iCloud Keychain en iTunes Store zijn dienstmerken van Apple Inc., die zijn gedeponeerd in de Verenigde Staten en andere landen. iOS is een handelsmerk of gedeponeerd handelsmerk van Cisco in de Verenigde Staten en andere landen dat in licentie wordt gebruikt. Andere product- en bedrijfsnamen die worden genoemd, kunnen handelsmerken zijn van hun respectieve eigenaars. Productspecificaties kunnen zonder voorafgaande kennisgeving worden gewijzigd. Dit materiaal wordt uitsluitend aangeboden ter informatie. Apple aanvaardt geen enkele aansprakelijkheid met betrekking tot het gebruik van deze informatie. April 2018