Bijlage Bescherming van persoonsgegevens voor Producten en Diensten van Microsoft

Laatst bijgewerkt 22 mei 2026

Contents

Overzicht van wijzigingen 2
Inleiding 3
Toepasselijke BBP-bepalingen en updates 3
Elektronische kennisgevingen 4
Eerdere versies 4
Definities 5
Algemene Voorwaarden 8
Naleving van wetten 8
Bepalingen inzake de bescherming van persoonsgegevens 8
Reikwijdte 8
Aard van de gegevensverwerking; eigendom 9
Bekendmaking van verwerkte gegevens 11
Verwerking van persoonsgegevens; AVG 12
Gegevensbeveiliging 15
Kennisgeving van beveiligingsincidenten 18
Gegevensoverdracht en locatie 19
Bewaring en verwijdering van gegevens 20
EU-gegevenswet 21
Geheimhoudingsplicht van de verwerker 21
Kennisgeving en maatregelen betreffende het gebruik van Subverwerkers 22

Previews ... 23
Onderwijsinstellingen ... 24
CJIS Klantovereenkomst ... 25
Zakenpartner HIPAA ... 25
Telecommunicatiegegevens ... 25
California Consumer Privacy Act (CCPA) ... 26
Biometrische Gegevens ... 26
Aanvullende Professionele Diensten ... 26
Contact opnemen met Microsoft ... 27
Bijlage A – Beveiligingsmaatregelen ... 28
Domein ... 28
Praktijken ... 28
Bijlage B – Betrokkenen en categorieën van persoonsgegevens ... 33
Bijlage C – Bijlage voor aanvullende waarborgen ... 36
Bijlage D – Bezwaren tegen een bevel of bindende wettelijke verplichting tot opschorting van Online Diensten ... 39
Bijlage 1 – Voorwaarden van de Algemene Verordening Gegevensbescherming van de Europese Unie ... 40
Relevante AVG-verplichtingen: Artikelen 5, 28, 32 en 33 ... 40

Overzicht van wijzigingen

22-5-2026 – In het artikel 'Kennisgeving en maatregelen betreffende het gebruik van Subverwerkers' is een verduidelijking toegevoegd betreffende subverwerkers die functionaliteit voor kunstmatige intelligentie ondersteunen.

Inleiding

De partijen gaan ermee akkoord dat deze Bijlage Bescherming van persoonsgegevens voor Producten en Diensten van Microsoft ("BBP") hun respectieve verplichtingen beschrijven met betrekking tot de verwerking en beveiliging van Klantgegevens, Gegevens van Professionele Diensten en Persoonsgegevens in verband met de Producten en Diensten. De BBP is door middel van verwijzing opgenomen in de Productvoorwaarden en andere Microsoft-overeenkomsten. De partijen gaan tevens ermee akkoord dat deze BBP van toepassing is op de verwerking en beveiliging van Gegevens van Professionele Diensten, tenzij een afzonderlijke overeenkomst voor de Professionele Diensten bestaat. Voor het gebruik van Niet-Microsoft-Producten gelden afzonderlijke voorwaarden, waaronder verschillende privacy- en beveiligingsbepalingen.

In het geval van strijdigheid of inconsistentie tussen de Voorwaarden in de BBP en andere voorwaarden in de Volume licentieovereenkomst van de Klant of andere toepasselijke overeenkomsten in verband met Producten en Diensten ("overeenkomst van de Klant"), prevaleren de Voorwaarden van de BBP. De bepalingen in de Voorwaarden van de BBP hebben voorrang boven eventuele strijdige bepalingen in de Privacyverklaring van Microsoft die anders van toepassing zijn op de verwerking van Klantgegevens, Persoonsgegevens of Gegevens van Professionele Diensten of Persoonsgegevens zoals gedefinieerd in dit document.

Microsoft neemt de verplichtingen in deze BBP op zich ten aanzien van alle klanten met een bestaande overeenkomst van de Klant. Deze verplichtingen zijn bindend voor Microsoft ten aanzien van de Klant, ongeacht (1) de Productvoorwaarden die overigens van toepassing zijn op een gegeven

Toepasselijke BBP-bepalingen en updates

Beperkingen betreffende updates

Wanneer de Klant een abonnement op een Product verlengt, een nieuw abonnement aanschaft, of een werkopdracht voor een Professionele Dienst aangaat, zijn de voorwaarden van de op dat moment geldende BBP van toepassing en worden deze niet gewijzigd tijdens het abonnement van de Klant voor dat Product of de looptijd van de Professionele Dienst. Wanneer de Klant een eeuwigdurende licentie voor Software verkrijgt, zijn de voorwaarden van de op dat moment geldende BBP van toepassing (met inachtneming van dezelfde bepaling voor het bepalen van de op dat moment geldende Productvoorwaarden voor die Software in de overeenkomst van de Klant) en worden deze niet gewijzigd tijdens de looptijd van de licentie van de Klant voor de betreffende Software.

Nieuwe functies, aanvullingen of verwante software

Niettegenstaande de voorgaande beperkingen betreffende updates, wanneer Microsoft functies, aanbiedingen, aanvullingen of verwante software introduceert die nieuw zijn (dat wil zeggen, die eerder niet bij de Producten of Diensten waren inbegrepen), kan Microsoft wat betreft het gebruik van deze functies, aanvullingen of verwante software door de Klant daarvoor voorwaarden voorschrijven of de BBP aanpassen. Indien aan deze voorwaarden wezenlijk nadelige wijzigingen in de Voorwaarden van de BBP zijn verbonden, geeft Microsoft de Klant de optie de nieuwe functies, aanbiedingen, aanvullingen of verwante software niet te gebruiken, zonder verlies van bestaande functionaliteit van algemeen beschikbare Producten of Professionele Diensten. Als de Klant de nieuwe functies, aanbiedingen, supplementen of verwante software niet installeert of gebruikt, zijn de corresponderende nieuwe voorwaarden niet van toepassing.

Voorschriften en vereisten van de overheid

Niettegenstaande de voorgaande beperkingen betreffende updates, kan Microsoft een Product of Professionele Dienst wijzigen of beëindigen in elk land of rechtsgebied waarin een huidige of toekomstige vereiste of verplichting van de overheid geldt die (1) Microsoft onderwerpt aan regelgeving of vereisten die niet in het algemeen van toepassing zijn op bedrijven die daar actief zijn, (2) het Microsoft lastig maken het Product of de Professionele Dienst zonder wijzigingen aan te bieden en/of (3) Microsoft doen geloven dat de Voorwaarden van de BBP of het Product of de Professionele Dienst in strijd zijn met een dergelijke vereiste of verplichting.

Elektronische kennisgevingen

Microsoft kan de Klant via elektronische weg informatie en mededelingen geven over Producten en Diensten, waaronder via e-mail, via het portaal voor een Online Dienst, of via een door Microsoft aangewezen website. Kennisgeving geldt vanaf de datum waarop deze beschikbaar is gemaakt door Microsoft.

Eerdere versies

De Voorwaarden in de BBP bevatten voorwaarden voor Producten en Diensten die op dit moment beschikbaar zijn. Voor eerdere versies van de Voorwaarden van de BBP kan de Klant https://aka.ms/licensingdocs raadplegen of contact opnemen met zijn reseller of Microsoft Account Manager.

Definities

Termen die in deze BBP met een hoofdletter worden geschreven maar hierin niet worden gedefinieerd, hebben de betekenis die eraan wordt gegeven in de overeenkomst van de Klant. In deze BBP worden de volgende gedefinieerde termen gebruikt:

"Klantgegevens" betekent alle gegevens, met inbegrip van alle tekst-, geluids-, video- en afbeeldingbestanden en software die aan Microsoft zijn verstrekt door, of uit naam van, de Klant door middel van het gebruik van de Online Dienst door de Klant. Gegevens van Professionele Diensten behoren niet tot Klantgegevens.

"Vereisten voor Bescherming van Persoonsgegevens" betekent de AVG, Lokale Wetgeving inzake Gegevensbescherming van de EU/EER, en toepasselijke wetten, voorschriften en andere wettelijke vereisten met betrekking tot (a) privacy en gegevensbeveiliging en (b) het gebruiken, verzamelen, bewaren, opslaan, beveiligen, bekendmaken, overdragen, verwijderen en anderszins verwerken van Persoonsgegevens.

"Voorwaarden van de BBP" betekent de voorwaarden in de BBP en eventuele Productspecifieke voorwaarden voor een Product in de Productvoorwaarden die de privacy- en beveiligingsvoorwaarden in de BBP voor een specifiek Product (of een functie van een Product) specifiek aanvullen of wijzigen. In het geval van strijdigheid of inconsistentie tussen de BBP en dergelijke Productspecifieke voorwaarden, prevaleren de Productspecifieke voorwaarden met betrekking tot het toepasselijke Product (of de functie van de Product).

"EU-klant" betekent een klant met een factuuradres in de Europese Economische Ruimte ("EER").

Onder "EU-gegevenswet" wordt verstaan Verordening (EU) 2023/2854 van het Europees Parlement en de Raad van 13 december 2023 betreffende geharmoniseerde regels voor eerlijke toegang tot en gebruik van gegevens en tot wijziging van Verordening (EU) 2020/1828 (Gegevenswet).

De dienst "Europese Dataverordening" betekent een Online Dienst die in licentie is gegeven aan een EU-klant, met uitzondering van een Online Dienst waarvoor de EU-klant ervoor heeft gekozen om Klantgegevens buiten de EER op te slaan.

"Exporteerbare gegevens en digitale activa" (EDDA) betekent klantgegevens. Voor de duidelijkheid: EDDA omvat geen bedrijfsgeheimen of intellectueel eigendom van Microsoft of gegevens die de beveiliging of integriteit van de Online Diensten in gevaar kunnen brengen.

"AVG" betekent de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming).

"Lokale Wetgeving inzake Gegevensbescherming van de EU/EER" betekent secundaire wetten en voorschriften voor de tenuitvoerlegging van de AVG.

"AVG-voorwaarden" betekent de bepalingen in Bijlage 1 op grond waarvan Microsoft bindende verplichtingen aangaat betreffende de verwerking van Persoonsgegevens door Microsoft, zoals vereist op grond van artikel 28 van de AVG.

"Persoonsgegevens" betekent alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

'Previewgegevens' betekent Klantgegevens en Persoonsgegevens die door of namens de Klant aan Microsoft zijn verstrekt via het gebruik van een Preview of die zijn gegenereerd via het gebruik van een Preview door de Klant.

'Product' heeft de betekenis die eraan wordt gegeven in de volumelicentieovereenkomst. Voor het gemak omvat "Product" ook Online Diensten en Software, elk zoals gedefinieerd in de volume licensing overeenkomst.

"Producten en Diensten" betekent Producten en Professionele Diensten. De beschikbaarheid van Producten en Professionele Diensten kan per regio verschillen en de toepasselijkheid van deze BBP op specifieke Producten en Professionele Diensten is onderworpen aan de beperkingen in het artikel Reikwijdte in deze BBP.

"Professionele Diensten" betekent de volgende diensten: (a) Adviesdiensten van Microsoft, bestaande uit diensten voor planning, advies, begeleiding, gegevensmigratie, implementatie en diensten voor de ontwikkeling van oplossingen/software op grond van een Werkopdracht voor Microsoft Enterprise Services of, indien overeengekomen in de Beschrijving van het Project, een Cloud Workload Acceleration Overeenkomst waarin deze BBP door middel van verwijzing is opgenomen; en (b) door Microsoft verleende technische ondersteuningsdiensten die klanten helpen bij het herkennen en oplossen van problemen die gevolgen hebben voor Producten, met inbegrip van technische

ondersteuning die wordt geleverd als onderdeel van Microsoft Unified Support of Premier Support Services en andere commerciële technische ondersteuningsdiensten. De Professionele Diensten omvatten niet de Producten of, uitsluitend binnen de context van de BBP, Aanvullende Professionele Diensten.

“Gegevens van Professionele Diensten” betekent alle gegevens, met inbegrip van tekst-, geluids-, video-, afbeeldings- of softwarebestanden die aan Microsoft worden verstrekt door of namens een Klant (of waarvoor de Klant een machtiging verleent aan Microsoft om deze op te halen in een Product) of overigens zijn verkregen of verwerkt door of namens Microsoft in het kader van een overeenkomst met Microsoft voor het verkrijgen van Professionele Diensten.

“Modelcontractbepalingen van 2021” betekent de standaardbepalingen voor gegevensbescherming (module verwerker-naar-verwerker) tussen Microsoft Ireland Operations Limited en Microsoft Corporation voor de overdracht van persoonsgegevens van verwerkers in de EER naar verwerkers die zijn gevestigd in derde landen die geen adequaat niveau van gegevensbescherming bieden, zoals beschreven in artikel 46 van de AVG en goedgekeurd door Besluit 2021/914/EC van de Europese Commissie van 4 juni 2021.

“Subverwerker” betekent de andere verwerkers die door Microsoft worden gebruikt voor het verwerken van Klantgegevens, Gegevens van Professionele Diensten en Persoonsgegevens, zoals beschreven in Artikel 28 van de AVG.

Met “overstappen” wordt de eenmalige overdracht van EDDA door een EU-klant vanuit een dienst Europese Dataverordening naar een cloudserviceprovider van een andere leverancier dan Microsoft bedoeld, die door de EU-klant is geïdentificeerd en waarvan de EU-klant de gegevens aan Microsoft verstrekt, of aan de on-premises ICT-omgeving van de EU-klant, wanneer de EU-klant het abonnement beëindigt en het gebruik van de dienst Europese Dataverordening beëindigt.

“Aanvullende Professionele Diensten” betekent ondersteuningsverzoeken die zijn doorverwezen door ondersteuning voor afhandeling door een team van Productengineering en andere advies- en ondersteuningsdiensten van Microsoft in verband met Producten of een volume licensing overeenkomst die niet zijn inbegrepen in de definitie van Professionele Diensten.

Termen die met een kleine letter worden geschreven, maar niet worden gedefinieerd in deze BBP, zoals 'inbreuk in verband met persoonsgegevens', 'verwerking', 'verwerkingsverantwoordelijke', 'verwerker', 'profilering', 'persoonsgegevens', en 'betrokkene', hebben dezelfde betekenis als beschreven in artikel 4 van de AVG, ongeacht of de AVG van toepassing is.

Algemene Voorwaarden

Naleving van wetten

Microsoft houdt zich aan alle wetten en voorschriften die van toepassing zijn op de levering van de Producten en Diensten, met inbegrip van toepasselijke wetgeving met betrekking tot het melden van een inbreuk op de beveiliging en de Vereisten voor Bescherming van Persoonsgegevens. Microsoft is echter niet verantwoordelijk voor naleving van wetten en voorschriften die van toepassing zijn op de Klant of de bedrijfstak van de Klant, maar die niet algemeen van toepassing zijn op leveranciers van informatietechnologiediensten. Microsoft bepaalt niet of gegevens van de Klant informatie bevatten die is onderworpen aan specifieke wetten of voorschriften. Alle Beveiligingsincidenten zijn onderworpen aan de onderstaande voorwaarden voor Kennisgevingen betreffende Beveiligingsincidenten.

De Klant moet voldoen aan alle wetten en voorschriften van toepassing op zijn gebruik van de Producten en Diensten, met inbegrip van wetgeving met betrekking tot biometrische gegevens, vertrouwelijkheid van communicatie, en de Vereisten voor Bescherming van Persoonsgegevens. De Klant is verantwoordelijk voor het bepalen of de Producten en Diensten geschikt zijn voor de opslag en verwerking van informatie op grond van specifieke wet- en regelgeving en voor het gebruik van de Producten en Diensten op een wijze die consistent is met de wettelijke en regulatieve verplichtingen van de Klant. De Klant is verantwoordelijk voor het reageren op elk verzoek van derden betreffende gebruik van de Producten en Diensten door de Klant, zoals een verzoek om inhoud te verwijderen op grond van de U.S. Digital Millennium Copyright Act of andere toepasselijke wetgeving.

Bepalingen inzake de bescherming van persoonsgegevens

Reikwijdte

De BBP-voorwaarden gelden voor alle Producten en Diensten, uitgezonderd zoals beschreven in dit gedeelte.

De BBP-voorwaarden zijn niet van toepassing op Producten of Professionele Diensten die in de Productvoorwaarden of de betreffende werkorder specifiek als uitgesloten worden aangeduid, of voor

zover deze zijn aangeduid als uitgesloten, en waarop de privacy- en beveiligingsvoorwaarden in de toepasselijke Productspecifieke of werkorderspecifieke voorwaarden van toepassing zijn.

Voor alle duidelijkheid: de BBP-voorwaarden zijn alleen van toepassing op de verwerking van gegevens in omgevingen onder het toezicht van Microsoft en diens subverwerkers. Hiertoe behoren gegevens die door Producten en Diensten naar Microsoft worden verzonden, maar niet gegevens die zich bij de Klant zelf bevinden of in de werkomgeving van een door de Klant geselecteerde externe derde partij.

Voor Aanvullende Professionele Diensten gaat Microsoft uitsluitend de verplichtingen aan die in het onderstaande artikel Aanvullende Professionele Diensten worden genoemd.

Aard van de gegevensverwerking; eigendom

Microsoft gebruikt en verwerkt Klantgegevens, Gegevens van Professionele Diensten en Persoonsgegevens uitsluitend zoals beschreven in en onderworpen aan de hieronder beschreven beperkingen (a) voor het leveren van de Producten en Diensten aan de Klant in overeenstemming met de gedocumenteerde instructies van de Klant, en (b) voor de zakelijke activiteiten in verband met de levering van de Producten en Diensten aan de Klant. Tussen partijen behoudt de Klant alle rechten, eigendom en belangen met betrekking tot de Klantgegevens en Gegevens van Professionele Diensten. Microsoft verkrijgt geen rechten met betrekking tot de Klantgegevens of Gegevens van Professionele Diensten, anders dan de rechten die de Klant in dit artikel aan Microsoft verleent. Deze paragraaf heeft geen invloed op de rechten van Microsoft met betrekking tot de software of diensten waarvoor Microsoft de Klant een licentie verleent.

Verwerking om de Producten en Diensten aan de Klant te leveren

Binnen de context van deze BBP bestaat het “leveren” van een Product uit:

- Het leveren van de functionele mogelijkheden, zoals gelicenseerd, geconfigureerd en gebruikt door de Klant en zijn gebruikers, met inbegrip van het leveren van een persoonlijke gebruikersbeleving;
- Probleemoplossing (problemen voorkomen, detecteren en verhelpen); en
- Producten up-to-date en effectief houden en de gebruikersproductiviteit, betrouwbaarheid, efficiëntie, kwaliteit en veiligheid verbeteren.

Binnen de context van deze BBP bestaat het “leveren” van Professionele Diensten uit:

- Levering van de Professionele Diensten, met inbegrip van technische ondersteuning, professionele diensten voor planning, advies, begeleiding, gegevensmigratie, implementatie en ontwikkeling van oplossingen/software.
- Probleemoplossing (problemen voorkomen, detecteren, onderzoeken, verlichten en verhelpen, met inbegrip van Beveiligingsincidenten en problemen die zijn vastgesteld in de Professionele Diensten of relevante Producten tijdens de levering van de Professionele Diensten); en
- Verbetering van de levering, functionaliteit, kwaliteit en beveiliging van Professionele Diensten en de onderliggende Producten op basis van problemen die zijn vastgesteld tijdens het leveren van Professionele Diensten, met inbegrip van het verhelpen van gebreken in de software, alsook de Producten en Diensten overigens up-to-date en performant te houden.

In elk geval wordt de levering van de Producten en Diensten uitgevoerd met het oog op de beveiligingsverplichtingen krachtens de Vereisten voor Bescherming van Persoonsgegevens in gedachten. Tijdens het leveren van Producten en Diensten, gebruikt of verwerkt Microsoft Klantgegevens, Gegevens van Professionele Diensten of Persoonsgegevens niet voor: (a) profilering van gebruikers, (b) adverteren of vergelijkbare commerciële doeleinden, of (c) marktonderzoek gericht op het creëren van nieuwe functionaliteit, diensten of producten of andere doeleinden, tenzij dergelijk gebruik of dergelijke verwerking in overeenstemming is met de gedocumenteerde instructies van de Klant.

Verwerking voor bedrijfsactiviteiten in het kader van de levering van de Producten en Diensten aan de Klant

Voor de doeleinden van deze BBP betekent “bedrijfsactiviteiten” de verwerkingsactiviteiten waarvoor de klant in dit artikel toestemming verleent.

De Klant verleent toestemming aan Microsoft om:

- bijeengevoegde statistische, niet-persoonlijke gegevens te creëren op basis van gegevens met gepseudonimiseerde identificatoren (zoals gebruikslogboeken met unieke, gepseudonimiseerde identificatoren); en
- statistieken te berekenen met betrekking tot Klantgegevens of Gegevens van Professionele Diensten

in beide gevallen zonder toegang tot, of analyse van, de inhoud van de Klantgegevens of Gegevens van Professionele Diensten en beperkt tot het bereiken van de onderstaande doeleinden, elk in het kader van de levering van Producten en Diensten aan de Klant.

Deze doeleinden zijn:

- facturering en accountbeheer;
- compensatie, zoals berekening van provisies van medewerkers en bonussen van partners;
- interne rapportage en bedrijfsmodellering, zoals prognoses, omzet, capaciteitsplanning en productstrategie; en
- financiële rapportage.

Bij de verwerking voor deze bedrijfsactiviteiten past Microsoft de principes van gegevensminimalisatie toe en worden Klantgegevens, Gegevens van Professionele Diensten of Persoonsgegevens niet gebruikt of anderszins verwerkt voor: (a) gebruikersprofilering, (b) adverteren of vergelijkbare commerciële doeleinden, of (c) voor enig ander doeleinde, afgezien van de doeleinden die in dit artikel worden vermeld. Verder blijft de verwerking voor bedrijfsactiviteiten, zoals bij elke verwerking op grond van deze BBP, onderworpen aan de geheimhoudingsverplichtingen en toezeggingen van Microsoft op grond van het artikel Bekendmaking van Verwerkte Gegevens.

Bekendmaking van verwerkte gegevens

Microsoft maakt geen Verwerkte Gegevens bekend en maakt deze niet toegankelijk, uitgezonderd: (1) op aanwijzing van de Klant; (2) zoals beschreven in deze BBP; of (3) indien wettelijk verplicht. Voor de doeleinden van dit artikel betekent "Verwerkte Gegevens": (a) Klantgegevens, (b) Gegevens van Professionele Diensten, (c) Persoonsgegevens en (d) andere gegevens die door Microsoft worden verwerkt in verband met de Producten en Diensten die vertrouwelijke gegevens van de Klant zijn op grond van de overeenkomst van de Klant. Alle verwerking van Verwerkte Gegevens is onderworpen aan de geheimhoudingsplicht van Microsoft op grond van de overeenkomst van de Klant.

Microsoft maakt geen Verwerkte Gegevens bekend en verleent geen toegang daartoe aan opsporingsautoriteiten, tenzij wettelijk verplicht. Indien opsporingsautoriteiten contact opnemen met Microsoft om Verwerkte Gegevens op te vragen, probeert Microsoft hen door te verwijzen om die gegevens rechtstreeks bij de Klant op te vragen. Indien Microsoft is gehouden om Gegevens van Professionele Diensten bekend te maken of toegang daartoe te verlenen aan opsporingsautoriteiten, zal Microsoft de Klant onmiddellijk op de hoogte stellen en een kopie van de vordering verstrekken, tenzij dit wettelijk niet is toegestaan.

Bij ontvangst van ieder ander verzoek van derden om Verwerkte Gegevens, zal Microsoft de Klant onmiddellijk op de hoogte stellen, tenzij dit wettelijk niet is toegestaan. Microsoft zal het verzoek afwijzen, tenzij Microsoft wettelijk verplicht is aan het verzoek te voldoen. Indien het verzoek gegrond is, zal Microsoft proberen de derde partij door te verwijzen zodat deze de gegevens rechtstreeks bij de Klant op kan vragen.

Microsoft maakt Verwerkte Gegevens alleen bekend of toegankelijk zoals vereist door de wet, op voorwaarde dat de wetten en praktijken de essentie van de fundamentele rechten en vrijheden respecteren en niet verder gaan dan wat nodig en evenredig is in een democratische samenleving en, indien van toepassing, om een van de doelstellingen genoemd in artikel 23, lid 1, van de AVG.

Microsoft verstrekt het volgende niet aan derden: (a) directe, indirecte, algehele of onbeperkte toegang tot Verwerkte Gegevens; (b) de platformversleutelingssleutels die zijn gebruikt voor het beveiligen van de Verwerkte Gegevens of middelen om deze versleuteling te breken; of (c) toegang tot Verwerkte Gegevens indien Microsoft ervan op de hoogte is dat deze gegevens worden gebruikt voor andere doeleinden dan welke worden genoemd in het verzoek van de derde partij.

Ter ondersteuning van het bovenstaande, kan Microsoft de basiscontactgegevens van de Klant aan de derde partij verstrekken.

Verwerking van persoonsgegevens; AVG

Alle Persoonsgegevens die door Microsoft worden verwerkt in verband met het leveren van de Producten en Diensten, worden verkregen als onderdeel van ofwel (a) Klantgegevens, (b) Gegevens van Professionele Diensten, of (c) gegevens die zijn gegenereerd, afgeleid of verzameld door Microsoft, inclusief gegevens die naar Microsoft zijn verzonden als gevolg van het gebruik van op diensten gebaseerde functionaliteit door een Klant of door Microsoft verkregen van lokaal geïnstalleerde software. Persoonsgegevens die aan Microsoft zijn gegeven door of namens de Klant door middel van het gebruik van de Online Dienst zijn ook Klantgegevens. Persoonsgegevens die aan Microsoft zijn gegeven door of namens de Klant door middel van het gebruik van de Professionele Diensten zijn ook Gegevens van Professionele Diensten. Er kunnen gepseudonimiseerde identifiers zijn opgenomen in gegevens die door Microsoft worden verwerkt in verband met de levering van de Producten, en dat zijn ook Persoonsgegevens. Gepseudonimiseerde Persoonsgegevens, of persoonsgegevens die van identiteitskenmerken zijn ontdaan maar niet zijn geanonimiseerd, of Persoonsgegevens die zijn afgeleid van Persoonsgegevens, zijn ook Persoonsgegevens.

In zoverre Microsoft optreedt als verwerker of subverwerker van Persoonsgegevens onderworpen aan de AVG, zijn de AVG-voorwaarden uit Bijlage 1 van toepassing en wordt de taal in het artikellid ("Verwerking van persoonsgegevens; AVG") beschouwd als aanvullend:

Rollen en verantwoordelijkheden van de verwerker en de verwerkingsverantwoordelijke

De Klant en Microsoft komen overeen dat de Klant de verwerkingsverantwoordelijke en Microsoft de verwerker is met betrekking tot de Persoonsgegevens, uitgezonderd in gevallen waarin (a) de Klant

optreedt als verwerker van Persoonsgegevens, in welk geval Microsoft een subverwerker is, of (b) anders is bepaald in de Productspecifieke voorwaarden of deze BBP. Wanneer Microsoft optreedt als de verwerker of subverwerker van Persoonsgegevens, verwerkt Microsoft Persoonsgegevens uitsluitend op gedocumenteerde instructie van de Klant. De Klant gaat ermee akkoord dat de overeenkomst van de Klant (met inbegrip van deze BBP en eventuele toepasselijke updates) samen met de productdocumentatie en het gebruik en de configuratie van de functies van de Producten door de Klant, de volledige en definitieve gedocumenteerde instructies van de Klant aan Microsoft zijn voor de verwerking van Persoonsgegevens, of de documentatie van de Professionele Diensten en het gebruik van de Professionele Diensten door de Klant. Informatie over het gebruik en de configuratie van de Producten is te vinden op https://docs.microsoft.com (of een opvolgende locatie) of in een andere overeenkomst waarin deze BBP is opgenomen. Met eventuele aanvullende of alternatieve instructies moet akkoord worden gegaan volgens het proces voor het aanvullen van de overeenkomst van de Klant. In elk geval waarin de AVG van toepassing is en de Klant als verwerker fungeert, waarborgt de Klant aan Microsoft dat de instructies van de Klant, met inbegrip van de benoeming van Microsoft als verwerker of subverwerker, zijn geautoriseerd door de relevante verwerkingsverantwoordelijke.

Voor zover Microsoft Persoonsgegevens die zijn onderworpen aan de AVG gebruikt of anderszins verwerkt voor bedrijfsactiviteiten in verband met de levering van de Producten en Diensten aan de Klant, houdt Microsoft zich aan de verplichtingen van een onafhankelijke verwerkings-verantwoordelijke op grond van de AVG met betrekking tot dergelijk gebruik. Microsoft aanvaardt de aanvullende verantwoordelijkheden van een “verwerkingsverantwoordelijke” op grond van de AVG voor dergelijke verwerking om: (a) te handelen in overeenstemming met regulatieve vereisten, voor zover dit vereist is op grond van de AVG; en (b) meer transparantie te bieden aan Klanten en de toerekenbaarheid van Microsoft voor dergelijke verwerking te bevestigen. Microsoft hanteert veiligheidsmaatregelen om Klantgegevens, Gegevens van Professionele Diensten en Persoonsgegevens die op dergelijke wijze worden verwerkt te beschermen, met inbegrip van de maatregelen die worden genoemd in deze BBP en die worden besproken in artikel 6, lid 4 van de AVG. Met betrekking tot de verwerking van Persoonsgegevens op grond van deze paragraaf gaat Microsoft de toezeggingen na die zijn uiteengezet in de sectie aanvullende waarborgen; voor die doeleinden wordt (i) elke openbaarmaking van persoonsgegevens door Microsoft, zoals beschreven in de sectie aanvullende waarborgen, die is overgedragen in verband met bedrijfsactiviteiten, beschouwd als een “Relevante openbaarmaking” en (ii) zijn de toezeggingen in de sectie aanvullende waarborgen van toepassing op dergelijke Persoonsgegevens.

Verwerkingsdetails

De partijen erkennen en gaan akkoord met het volgende:

- **Onderwerp.** Het onderwerp van de verwerking is beperkt tot Persoonsgegevens binnen de reikwijdte van het bovenstaande artikel "Aard van de gegevensverwerking; eigendom" in deze BBP en de AVG.
- **Duur van de verwerking.** De duur van de verwerking is overeenkomstig de instructies van de Klant en de voorwaarden van de BBP.
- **Aard en doeleinde van de verwerking.** De aard en het doel van de verwerking is de levering van de Producten en Diensten in het kader van de overeenkomst van de Klant en voor bedrijfsactiviteiten in verband met de levering van de Producten en Diensten aan de Klant (zoals verder beschreven in het artikel "Aard van de gegevensverwerking; eigendom", eerder in deze BBP).
- **Categorieën gegevens.** Tot de typen Persoonsgegevens die door Microsoft worden verwerkt in het kader van de levering van de Producten en Diensten behoren: (i) Persoonsgegevens die de Klant verkiest op te nemen in Klantgegevens en Gegevens van Professionele Diensten; en (ii) gegevens die uitdrukkelijk worden genoemd in artikel 4 van de AVG die door Microsoft kunnen worden gegenereerd, afgeleid of verzameld, met inbegrip van gegevens die naar Microsoft worden verzonden als gevolg van het gebruik door de Klant van op diensten services gebaseerde functionaliteit of die door Microsoft zijn verkregen uit lokaal geïnstalleerde software. De typen Persoonsgegevens die de Klant verkiest op te nemen in Klantgegevens en Gegevens van Professionele Diensten kunnen elk van de categorieën van Persoonsgegevens zijn die zijn aangeduid in een register dat wordt onderhouden door de Klant die optreedt als verwerkingsverantwoordelijke in de zin van artikel 30 van de AVG, met inbegrip van de categorieën Persoonsgegevens die worden beschreven in Bijlage B.
- **Betrokkenen.** De categorieën van betrokken zijn vertegenwoordigers en eindgebruikers van de Klant, zoals medewerkers, opdrachtnemers, partners en klanten. Hiertoe kunnen ook andere categorieën van betrokkenen behoren die zijn aangeduid in een register dat wordt onderhouden door de Klant die optreedt als verwerkingsverantwoordelijke in de zin van artikel 30 van de AVG, met inbegrip van de categorieën van betrokkenen die worden beschreven in Bijlage B.

Rechten van betrokkenen; assistentie bij verzoeken

Microsoft biedt de Klant de mogelijkheid, op een wijze die in overeenstemming is met de functionaliteit van de Producten en Diensten en de rol van Microsoft als verwerker, om te voldoen aan verzoeken van betrokkenen om hun rechten op grond van de AVG uit te oefenen. Indien Microsoft

een verzoek ontvangt van een betrokkene van de Klant om gebruik te maken van een of meer rechten op grond van de AVG in verband met de Producten en Diensten waarvoor Microsoft fungeert als gegevensverwerker of subverwerker, zal Microsoft de betrokkene doorverwijzen om het verzoek rechtstreeks aan de Klant te richten. De Klant is ervoor verantwoordelijk te reageren op een dergelijk verzoek, onder andere door gebruik te maken van de functionaliteit van de Producten en Diensten, indien nodig. Microsoft zal voldoen aan redelijke verzoeken van de Klant om de Klant te helpen bij het beantwoorden van dergelijke verzoeken van een betrokkene.

Register van verwerkingsactiviteiten

Voor zover de AVG vereist dat Microsoft dossiers verzamelt en onderhoud met bepaalde informatie met betrekking tot de Klant, dient de Klant dergelijke informatie op verzoek aan Microsoft te verstrekken en deze nauwkeurig en up-to-date te houden. Microsoft kan dergelijke informatie beschikbaar maken voor een toezichthoudende instantie, indien dit wordt vereist door de AVG.

Gegevensbeveiliging

Veiligheidsmaatregelen en -beleid

Microsoft implementeert en onderhoudt gepaste technische en organisatorische maatregelen om de Klantgegevens, Gegevens van Professionele Diensten en Persoonsgegevens te beschermen tegen onvoorziene of onrechtmatige vernietiging, verlies en wijziging, of ongeautoriseerde bekendmaking van of toegang tot persoonsgegevens die worden verzonden of anderszins worden verwerkt. Deze maatregelen worden beschreven in een Microsoft Veiligheidsbeleid. Microsoft maakt dat beleid bekend aan de Klant, samen met andere informatie betreffende de beveiligingsmaatregelen en het beveiligingsbeleid van Microsoft waar de Klant redelijkerwijs om vraagt.

Deze maatregelen dienen ook te voldoen aan de vereisten die worden uiteengezet in ISO 27001, ISO 27002 en ISO 27018. Een beschrijving van de veiligheidsmaatregelen voor deze vereisten is verkrijgbaar voor Klanten.

Elke Core Online Dienst voldoet daarnaast aan de controlenormen en -kaders die worden vermeld in de tabel in de Productvoorwaarden. In elke Core Online Dienst en Professional Service worden de beveiligingsmaatregelen die zijn uiteengezet in Bijlage A voor de bescherming van Klantgegevens en Gegevens van Professionele Diensten geïmplementeerd en onderhouden.

Microsoft implementeert en handhaaft de beveiligingsmaatregelen die zijn uiteengezet in Bijlage II van de Modelcontractbepalingen 2021 voor de bescherming van Persoonsgegevens binnen de reikwijdte van de AVG.

Microsoft kan op elk moment industrie- en overheidsnormen toevoegen. Microsoft zal de normen ISO 27001, ISO 27002, ISO 27018 of normen of kaders in de tabel voor Core Online Diensten in de Productvoorwaarden niet loslaten, tenzij deze niet meer worden gebruikt binnen de sector en worden vervangen door opvolgende normen (indien van toepassing).

Gegevensversleuteling

Klantgegevens en Gegevens voor Professionele Diensten (elk met inbegrip van eventuele Persoonsgegevens) in transit over openbare netwerken tussen de Klant en Microsoft, of tussen Microsoft-datacentra, worden standaard versleuteld.

Microsoft versleutelt ook Klantgegevens in rust in Online Diensten en Gegevens van Professionele Diensten in rust. In het geval van Online Diensten op basis waarvan de Klant of een derde partij, die handelt namens de Klant, toepassingen kan bouwen (bijvoorbeeld bepaalde Azure Services), kan de Klant naar eigen goeddunken gebruikmaken van versleuteling van gegevens die in dergelijke toepassingen zijn opgeslagen, waarbij gebruik wordt gemaakt van mogelijkheden die door Microsoft worden geboden of die de Klant van derden heeft verkregen.

Toegang tot gegevens

Microsoft maakt gebruik van 'least privilege'-toegangsmechanismen voor het beheren van de toegang tot Klantgegevens en Gegevens van Professionele Diensten (met inbegrip van eventuele daarin opgenomen Persoonsgegevens). Er wordt gebruikgemaakt van op rollen gebaseerde toegangscontrole om erop toe te zien dat toegang tot Klantgegevens en Gegevens van Professionele Diensten, die nodig zijn voor de werking van de dienst, plaatsvindt voor een passend doeleinde met goedkeuring en toezicht van de beheerders. Voor Core Online Diensten en Professional Diensten onderhoudt Microsoft mechanismen voor toegangscontrole die worden beschreven in de tabel “Beveiligingsmaatregelen” in Bijlage A; en Microsoft-personeel heeft geen permanente toegang tot Klantgegevens en wordt eventuele vereiste toegang voor een beperkte tijd verleend.

Verantwoordelijkheden van de Klant

De Klant is geheel zelf verantwoordelijk voor de onafhankelijke vaststelling of de technische en organisatorische maatregelen voor Producten en Diensten voldoen aan de vereisten van de Klant, met inbegrip van de veiligheidsverplichtingen op grond van de toepasselijke Vereisten voor Bescherming van Persoonsgegevens. De Klant erkent en gaat ermee akkoord dat de veiligheidsmaatregelen en het veiligheidsbeleid die worden geïmplementeerd en onderhouden door Microsoft een mate van veiligheid bieden die in overeenstemming is met het risico dat aan de Persoonsgegevens is verbonden, rekening houdend met de stand van de techniek, de uitvoeringskosten, en de aard, omvang, context en doeleinden van de verwerking van de Persoonsgegevens, alsmede de risico's

voor individuele personen. De klant is verantwoordelijk voor de implementatie en het behoud van de privacybescherming en de veiligheidsmaatregelen voor componenten die de klant levert of beheert (zoals apparaten die zijn geregistreerd bij Microsoft Intune of binnen een virtuele Microsoft Azure-machine of -toepassing van de klant).

Nalevingscontrole

Microsoft voert controles uit van de beveiliging van de computers, de computeromgeving en de fysieke datacenters die worden gebruikt voor het verwerken van Klantgegevens, Gegevens van Professionele Diensten en Persoonsgegevens, en wel als volgt:

- Waar een norm of raamwerk voorziet in controles, wordt ten minste eenmaal per jaar een audit volgens deze norm of dit raamwerk uitgevoerd.
- Elke audit wordt uitgevoerd volgens de normen en regels van de regulatieve of goedkeurende instantie voor de betreffende controlenorm of het controleraamwerk.
- Elke audit wordt uitgevoerd door gekwalificeerde, onafhankelijke externe beveiligingscontroleurs die door Microsoft worden geselecteerd en betaald.

Elke audit resulteert in de opstelling van een auditrapport ("Microsoft-controlerapport"). Microsoft maakt deze rapporten beschikbaar ter inzage op https://servicetrust.microsoft.com/ of op een andere door Microsoft aangewezen locatie. Het Microsoft-auditrapport wordt beschouwd als Vertrouwelijke Informatie van Microsoft en bevat een duidelijke beschrijving van eventuele wezenlijke bevindingen van de auditeur. Microsoft zal kwesties die in het Microsoft-auditrapport worden vermeld direct verhelpen om te voldoen aan de eisen van de auditeur. Indien de Klant daarom vraagt, zal Microsoft elk Microsoft-auditrapport aan de Klant verstrekken. Voor het Microsoft-auditrapport gelden de geheimhoudings- en verspreidingsbeperkingen van Microsoft en de auditeur.

Voor zover redelijkerwijs niet kan worden voldaan aan de auditvereisten van de Klant op grond van de Vereisten voor Bescherming van Persoonsgegevens door middel van de auditrapporten, documentatie of nalevingsinformatie die Microsoft in het algemeen beschikbaar stelt aan klanten, zal Microsoft onverwijld reageren op aanvullende audit-instructies van de Klant. Voordat een audit wordt uitgevoerd, bereiken de Klant en Microsoft een wederzijdse overstemming over de reikwijdte, timing, duur, audit- en bewijsvereisten, en de kosten van de audit, mits deze vereiste tot overeenstemming er niet toe leidt dat Microsoft de uitvoering van de audit op onredelijke wijze kan vertragen. Voor zover dit noodzakelijk is voor het uitvoeren van de audit, maakt Microsoft de verwerkingssystemen, faciliteiten en ondersteunende documentatie die relevant zijn voor de verwerking van Klantgegevens, Gegevens van Professionele Diensten en Persoonsgegevens van Microsoft, haar Gelieerde Ondernemingen en haar Subverwerkers beschikbaar. Een dergelijke controle wordt uitgevoerd door

een onafhankelijk, erkend extern accountantskantoor tijdens normale kantooruren, met redelijke voorafgaande kennisgeving aan Microsoft en onderworpen aan redelijke geheimhoudingsprocedures. De Klant en de auditeur hebben geen toegang tot gegevens van andere klanten van Microsoft of tot systemen of faciliteiten van Microsoft die niet betrokken zijn bij de levering van de toepasselijke Producten en Diensten. De Klant is verantwoordelijk voor alle kosten verbonden aan een dergelijke audit, met inbegrip van alle redelijke kosten voor de tijd die Microsoft besteedt aan een dergelijke audit, naast de tarieven voor de diensten die door Microsoft worden uitgevoerd. Als het auditrapport dat wordt gegenereerd naar aanleiding van de auditvan de Klant bevindingen bevat van wezenlijke niet-naleving, dient de Klant het auditrapport te delen met Microsoft en zal Microsoft eventuele wezenlijke niet-naleving onverwijld verhelpen.

Niets in dit gedeelte van de BBP houdt een afwijking of aanpassing van de AVG-voorwaarden in of heeft gevolgen voor de rechten van toezichthoudende instanties of betrokkenen op grond van de Vereisten voor Bescherming van Persoonsgegevens. Microsoft Corporation is een beoogde derde begunstigde van dit artikel.

Kennisgeving van beveiligingsincidenten

Indien Microsoft kennis heeft van een schending van de beveiliging die leidt tot, hetzij per ongeluk hetzij onrechtmatig, de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot Klantgegevens, Gegevens van Professionele Diensten of Persoonsgegevens die op dat moment door Microsoft worden verwerkt (elk een "Beveiligingsincident"), zal Microsoft onverwijld en zonder onnodige vertraging (1) de Klant op de hoogte stellen van het Beveiligingsincident; (2) het Beveiligingsincident onderzoeken en de Klant voorzien van gedetailleerde informatie over het Beveiligingsincident; en (3) redelijke stappen nemen om de gevolgen te beperken en de schade die voortkomt uit het Beveiligingsincident te beperken.

Kennisgeving(en) van Beveiligingsincidenten worden geleverd aan de Klant langs een door Microsoft gekozen weg, waaronder via e-mail. Het is de volledig eigen verantwoordelijkheid van de Klant om erop toe te zien dat de contactgegevens waarover Microsoft beschikt voor elk toepasselijk Product en elke Toepasselijke Professionele Dienst altijd up-to-date zijn. De Klant is geheel zelf verantwoordelijk voor de naleving van zijn verplichtingen op grond van de wetten inzake kennisgeving van incidenten die van toepassing zijn op de Klant en de nakoming van zijn verplichtingen met betrekking tot de kennisgeving van Beveiligingsincidenten aan derden.

Microsoft zal redelijke inspanningen verrichten om de Klant te helpen bij de nakoming van de verplichtingen van de Klant op grond van artikel 33 van de AVG of andere toepasselijke wetten of

voorschriften om de relevante toezichthoudende autoriteit en de betrokkenen op de hoogte te stellen van een dergelijk Beveiligingsincident.

De kennisgeving van of reactie op een Beveiligingsincident door Microsoft is geen erkenning van Microsoft van enig gebrek of aansprakelijkheid met betrekking tot het Beveiligingsincident.

De Klant dient Microsoft onmiddellijk op de hoogte te stellen van mogelijk misbruik van de accounts of verificatiegegevens van de Klant of beveiligingsincidenten in verband met de Producten en Diensten.

Gegevensoverdracht en locatie

Gegevensoverdracht

Klantgegevens, Gegevens van Professionele Diensten en Persoonsgegevens die Microsoft namens de Klant verwerkt, mogen niet worden overgedragen aan, of opgeslagen en verwerkt op een geografische locatie, uitgezonderd in overeenstemming met de Voorwaarden van de BBP en de waarborgen die hieronder in dit artikel worden beschreven. Rekening houdend met dergelijke waarborgen, machtigt de Klant Microsoft om Klantgegevens, Gegevens van Professionele Diensten en Persoonsgegevens over te dragen naar de Verenigde Staten of enig ander land waarin Microsoft of haar Subverwerkers actief zijn en om Klantgegevens en Persoonsgegevens op te slaan en te verwerken voor het leveren van de Producten, behalve zoals elders in de Voorwaarden van de BBP is beschreven.

Elke overdracht van Klantgegevens, Gegevens van Professionele Diensten en Persoonsgegevens buiten de Europese Unie, de Europese Economische Ruimte, het Verenigd Koninkrijk en Zwitserland ten behoeve van de levering van de Producten en Diensten is onderworpen aan de Modelcontractbepalingen van 2021 die door Microsoft zijn geïmplementeerd. Bovendien zijn overdrachten vanuit het Verenigd Koninkrijk onderworpen aan de door Microsoft geïmplementeerde IDTA. Binnen de context van deze BBP betekent de “IDTA” het International Data Transfer Addendum bij de modelcontractbepalingen voor internationale gegevensoverdracht van de Europese Commissie, uitgegeven door het UK Information Commissioner's Office onder S119A(1) van de UK Data Protection Act 2018. Microsoft houdt zich aan de vereisten van de wetgeving inzake bescherming van persoonsgegevens van de Europese Economische Ruimte, het Verenigd Koninkrijk en Zwitserland betreffende het verzamelen, gebruiken, overdragen, bewaren en op overige wijze verwerken van Persoonsgegevens uit de Europese Economische Ruimte, het Verenigd Koninkrijk en Zwitserland. Alle overdrachten van Persoonsgegevens naar een derde land of een internationale organisatie zijn onderworpen zijn aan passende veiligheidsmechanismen, zoals beschreven in artikel 46 van de AVG, en dergelijke overdrachten en veiligheidsmechanismen worden gedocumenteerd overeenkomstig artikel 30, lid 2 van de AVG.

Verder is Microsoft gecertificeerd in het kader van het gegevensprivacyraamwerk tussen de EU en de VS en tussen Zwitserland en de VS en de uitbreiding van het gegevensprivacyraamwerk tussen de EU en de VS voor het Verenigd Koninkrijk, en de verplichtingen die hieraan zijn verbonden. Microsoft gaat ermee akkoord de Klant op de hoogte te stellen indien Microsoft tot de vaststelling komt dat Microsoft niet meer kan voldoen aan haar verplichting om dezelfde mate van bescherming te bieden als op grond van de beginselen van het gegevensprivacyraamwerk vereist is.

Locatie van Klantgegevens

In het geval van Core Online Diensten slaat Microsoft Klantgegevens at-rest op in bepaalde grote geografische gebieden (elk een Geo), zoals beschreven in de Productvoorwaarden.

In het geval van Diensten waarvoor de EU Data Boundary geldt, zal Microsoft Klantgegevens en Persoonsgegevens opslaan en verwerken en Gegevens van Professionele Diensten at-rest opslaan binnen de Europese Unie en de Europese Vrijhandelsassociatie (EVA), zoals beschreven in de Productvoorwaarden.

Microsoft legt geen controles of beperkingen op aan de regio's waarvandaan de Klant of de eindgebruikers van de Klant Klantgegevens kunnen raadplegen of verplaatsen.

Bewaring en verwijdering van gegevens

Op ieder moment gedurende de looptijd van het abonnement van de Klant of de toepasselijke werkovereenkomst voor Professionele Diensten heeft de Klant de mogelijkheid Klantgegevens die zijn opgeslagen in elke Online Dienst en Gegevens van Professionele Diensten te raadplegen, op te halen en te verwijderen.

Uitgezonderd in het geval van gratis evaluatieversies en LinkedIn-diensten, bewaart Microsoft Klantgegevens die achterblijven in de Online Dienst gedurende 90 dagen vanaf het vervallen of beëindigen van het abonnement van de Klant in een account met beperkte functionaliteit, zodat de Klant de gegevens kan ophalen. Nadat de bewaarperiode van 90 dagen is verstreken, heft Microsoft het account van de Klant op en verwijdert Microsoft de Klantgegevens en Persoonsgegevens die zijn opgeslagen in Online Diensten binnen nog eens 90 dagen, tenzij deze BBP het recht geeft om de gegevens te bewaren.

In het geval van Persoonsgegevens in verband met de Software en Gegevens van Professionele Diensten verwijdert Microsoft alle exemplaren nadat de zakelijke doeleinden waarvoor de gegevens werden verzameld of overgedragen zijn vervuld, of eerder, op verzoek van de Klant, tenzij Microsoft op grond van deze BBP gerechtigd is de gegevens te bewaren.

De Online Dienst ondersteunt mogelijk niet het bewaren of ophalen van software die door de Klant wordt verstrekt. Microsoft is niet aansprakelijk voor het verwijderen van Klantgegevens, Gegevens van Professionele Diensten of Persoonsgegevens, zoals beschreven in dit artikel.

EU-gegevenswet

Overstappen is op elk gewenst moment toegestaan zonder extra kosten, afgezien van de vergoedingen en andere bedragen die anderszins verschuldigd zijn krachtens de overeenkomst met de EU-klant. EU-klanten mogen op elk gewenst moment EDDA raadplegen, exporteren en verwijderen, en dit geldt ook voor EDDA tot 90 dagen na beëindiging van het abonnement, zoals vastgelegd in de bepaling Gegevensbehoud en -verwijdering. EU-klanten beslissen zelf wanneer ze beginnen met het exporteren van EDDA en op welke termijn. Het kan langer dan 30 dagen duren voordat de EDDA daadwerkelijk door een EU-klant wordt geëxtraheerd en geëxporteerd, afhankelijk van de specifieke configuratie van de klant, de hoeveelheid gegevens, de overstapbestemming en andere omstandigheden waarover Microsoft geen controle heeft. EU-klanten dienen de overstap te voltooien vóór beëindiging van de dienst Europese Dataverordening. EU-klanten kunnen dit doen door Microsoft 60 dagen van tevoren op de hoogte te stellen en het bedrag te betalen dat nog verschuldigd is op grond van de overeenkomst van de EU-klant. Microsoft zal redelijke assistentie verlenen bij het overstappen en zal de nodige zorgvuldigheid betrachten zoals uiteengezet in de Gegevensbeveiliging en andere secties van de Gegevensbeschermingsovereenkomst en conform de overeenkomst van de Klant bij het leveren van de diensten voor Europese Dataverordening tijdens het overstappen en bij parallel gebruik. Een EU-klant kan korting krijgen op de kosten voor dataverkeer die verband houden met het overstappen en parallel gebruik, zoals bepaald in de wet. Deze voorwaarden voor de EU-gegevenswet zijn niet van toepassing op previews.

Ondersteunende materialen over gegevensexport en methoden en informatie met betrekking tot de Microsoft ICT-infrastructuur die wordt gebruikt om diensten voor Europese Dataverordening te leveren en hoe Microsoft reageert op verzoeken van de overheid om toegang tot gegevens, vindt u in de Productvoorwaarden.

Geheimhoudingsplicht van de verwerker

Microsoft zal erop toezien dat het personeel dat wordt ingezet voor de verwerking van Klantgegevens, Gegevens van Professionele Diensten of Persoonsgegevens (i) deze uitsluitend zal verwerken op aanwijzing van de Klant of zoals beschreven in deze BBP, en (ii) verplicht zal zijn de vertrouwelijkheid en veiligheid van de gegevens te bewaken, ook nadat de werkovereenkomst met hen is geëindigd. Microsoft zal een periodiek en verplicht trainings- en bewustzijnsprogramma inzake

persoonsgegevens bescherming en -beveiliging bieden aan het personeel dat toegang heeft tot Klantgegevens, Gegevens van Professionele Diensten en Persoonsgegevens, overeenkomstig de toepasselijke regelgeving over bescherming van persoonsgegevens en binnen de sector geldende normen.

Kennisgeving en maatregelen betreffende het gebruik van Subverwerkers

Microsoft kan Subverwerkers inhuren om namens Microsoft bepaalde beperkte of aanvullende diensten te leveren. De Klant stemt in met dit inhuren en met Gelieerde Ondernemingen van Microsoft als Subverwerkers. De bovenstaande autorisaties vormen de voorafgaande schriftelijke toestemming van de Klant voor de uitbesteding van de verwerking van Klantgegevens, Gegevens van Professionele Diensten en Persoonsgegevens door Microsoft indien deze toestemming is vereist op grond van de Modelcontractbepalingen of de AVG-voorwaarden.

Microsoft is verantwoordelijk voor de naleving van de verplichtingen van Microsoft op grond van deze BBP door de Subverwerkers. Microsoft maakt informatie over Subverwerkers beschikbaar op een Microsoft-website. Wanneer Microsoft een Subverwerker inschakelt, zal Microsoft door middel van een schriftelijk contract ervoor zorgen dat de Subverwerker de Klantgegevens, Gegevens van Professionele Diensten of Persoonsgegevens uitsluitend mag raadplegen en gebruiken voor het leveren van de diensten waarvoor Microsoft de Subverwerker heeft ingehuurd en de Klantgegevens, Gegevens van Professionele Diensten en Persoonsgegevens voor geen enkel ander doel mag gebruiken. Microsoft zal erop toezien dat Subverwerkers zijn gebonden door schriftelijke overeenkomsten die hen verplichten ten minste dezelfde mate van bescherming van persoonsgegevens te bieden als welke van Microsoft wordt verlangd op grond van de BBP, met inbegrip van de beperkingen betreffende verstrekking van Verwerkte Gegevens. Microsoft gaat ermee akkoord toezicht te houden op de Subverwerkers om erop toe te zien dat aan deze contractuele verplichtingen wordt voldaan.

Zo nu en dan kan Microsoft nieuwe Subverwerkers inschakelen. Microsoft stelt de Klant hiervan vooraf op de hoogte en zal, voor zover van toepassing, de website bijwerken en de Klant een mechanisme bieden om ten minste 6 maanden voordat een nieuwe Subverwerker toegang wordt verleend tot Gegevens van de Klant op de hoogte te worden gesteld van het nieuws betreffende de nieuwe Subverwerker. Voor subverwerkers die functionaliteit voor kunstmatige intelligentie ondersteunen, bedraagt deze termijn 30 dagen, met de mogelijkheid om het gebruik van de betreffende subverwerker tot ten minste 6 maanden na de kennisgeving uit te schakelen. Verder zal

Microsoft ten minste 30 dagen voordat aan die Subverwerker toegang wordt verleend tot Gegevens van Professionele Diensten of Persoonsgegevens, anders dan welke zijn opgenomen in Klantgegevens, de Klant in kennis stellen en, indien van toepassing, de website bijwerken en voorzien in een mechanisme om de Klant op de hoogte te stellen van de bijgewerkte inhoud op de website. Indien Microsoft voor een nieuw Product of nieuwe Professionele Dienst een nieuwe Subverwerker inschakelt die Klantgegevens, Gegevens van Professionele Diensten of Persoonsgegevens verwerkt, stelt Microsoft de Klant hiervan op de hoogte voordat het Product of de Professionele Dienst beschikbaar komt.

Indien de Klant een nieuwe Subverwerker voor een Online Dienst of Professionele Dienst niet goedkeurt, mag de Klant abonnementen voor de toepasselijke Online Dienst of de toepasselijke Dienstenspecificaties voor de toepasselijke Professionele Dienst zonder boete of opzegkosten opzeggen door voor het einde van de relevante kennisgevingsperiode een schriftelijke kennisgeving van opzegging in te dienen. Indien de Klant een nieuwe Subverwerker voor Software niet goedkeurt, en de Klant het gebruik van de Subverwerker redelijkerwijs niet kan vermijden door de verwerking van gegevens door Microsoft te beperken, zoals uiteengezet in de documentatie of in deze BBP, mag de Klant de licentie voor het betreffende softwareproduct zonder boete opzeggen door voor het einde van de relevante kennisgevingstermijn een schriftelijke kennisgeving van opzegging in te dienen. De Klant kan samen met de kennisgeving van opzegging ook een uitleg van de redenen voor het niet verlenen van de goedkeuring indienen om Microsoft in staat te stellen de aanstelling van een dergelijke nieuwe Subverwerker te heroverwegen op basis van de toepasselijke bedenkingen. Indien de betrokken Product deel uitmaakt van een suite (of vergelijkbare enkelvoudige aanschaf van diensten), geldt de opzegging voor de volledige suite. Na opzegging schrapt Microsoft de betalingsverplichtingen voor abonnementen of andere toepasselijke onbetaalde werkzaamheden met betrekking tot de opgezegde Producten of Diensten van de daaropvolgende facturen aan de Klant of de reseller van de Klant.

Previews

Bij Previews wordt mogelijk gebruikgemaakt van minder of andere privacy- en veiligheidsmaatregelen dan welke doorgaans worden gebruikt voor de Producten en Diensten. Tenzij anders aangegeven, mag de Klant Previews niet gebruiken voor het verwerken van Persoonsgegevens of andere gegevens die zijn onderworpen aan wettelijke of regulatieve nalevingsvereisten. Met uitzondering van Previews die verwerking van persoonsgegevens toestaan, zijn de volgende voorwaarden in deze BBP niet van toepassing op Previews: Verwerking van Persoonsgegevens; AVG, Gegevensbeveiliging en Zakenpartner HIPAA. In het geval van Professionele Diensten voldoen aanbiedingen die zijn

aangeduid als Previews of Beperkte Release, alleen aan de voorwaarden voor Aanvullende Professionele Diensten.

Voor Previews die verwerking van Persoonsgegevens toestaan, zijn alle voorwaarden in deze BBP van toepassing, onder voorbehoud van het volgende:

- Previewgegevens kunnen worden overgedragen naar en opgeslagen en verwerkt in de Verenigde Staten en andere landen waarin Microsoft of haar Subverwerkers werkzaam zijn. Bijgevolg is de Locatie van Klantgegevens niet van toepassing op Previews voor zover het de landen zou beperken waarin Microsoft Previewgegevens kan overdragen, opslaan of verwerken.
- Previews mogen Previewgegevens niet langer bewaren dan de duur van een Preview. Wanneer een Preview eindigt of de Klant anderszins stopt met deelname aan een Preview, kan Microsoft Previewgegevens verwijderen, zelfs als de Preview vervolgens algemeen commercieel beschikbaar wordt gesteld. Dienovereenkomstig is Gegevensbehoud- en verwijdering niet van toepassing op Previews voor zover het het recht van Microsoft om Previewgegevens te verwijderen, zou beperken.

Voor Previews kunnen aanvullende voorwaarden gelden, die afzonderlijk als onderdeel van de Previews worden vermeld.

Onderwijsinstellingen

Indien de Klant een onderwijsbureau of -instelling is waarop de regels van de Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (FERPA) van toepassing zijn, verklaart Microsoft dat Microsoft, in het kader van de doeleinden van de BBP, wordt beschouwd als “schoolfunctionaris” met “legitieme educatieve belangen” in Klantgegevens en Gegevens van Professionele Diensten, zoals deze termen worden gedefinieerd in FERPA en de regelgeving ter implementatie hiervan, en Microsoft stemt ermee in zich te houden aan de beperkingen en vereisten die door 34 CFR 99.33(a) worden opgelegd aan schoolfunctionarissen.

De Klant begrijpt dat Microsoft nauwelijks of niet beschikt over contactgegevens van de studenten van de Klant en de ouders van studenten. Daarom is de Klant verantwoordelijk voor het verkrijgen van toestemming van de ouders voor het gebruik van de Producten en Diensten door de eindgebruiker, voor zover dergelijke toestemming vereist is op grond van het toepasselijk recht, en zal de Klant studenten (of, bij studenten jonger dan 18 jaar die geen onderwijs volgen aan een hogeronderwijsinstelling, de ouders van de student) namens Microsoft op de hoogte stellen van een gerechtelijk bevel of wettig uitgebrachte dagvaarding waarin de openbaarmaking van Klantgegevens

en Gegevens van Professionele Diensten in het bezit van Microsoft wordt geëist, waar dit op grond van het toepasselijk recht verplicht is.

CJIS Klantovereenkomst

Microsoft levert bepaalde clouddiensten ("Clouddiensten") voor overheidsinstellingen overeenkomstig het veiligheidsbeleid ("CJIS Beleid") van de FBI met betrekking tot de Strafrechtelijke Informatie Services ("CJIS"). Het CJIS Beleid is van toepassing op het gebruik en de overdracht van strafrechtelijke informatie. Alle diensten van Microsoft die vallen onder de CJIS worden beheerst door de voorwaarden in de CJIS Management Agreement.

Zakenpartner HIPAA

Als de Klant een "onder de voorwaarden vallende entiteit" of een "zakenpartner" is en "beschermde gezondheidsinformatie" opneemt in Klantgegevens of Gegevens van Professionele Diensten, zoals deze termen zijn gedefinieerd in de Health Insurance Portability and Accountability Act uit 1996, inclusief amendementen, en de op grond hiervan afgekondigde regelgeving (samen, de "HIPAA"), omvat de uitvoering van de overeenkomst van de Klant de uitvoering van de Overeenkomst zakenpartner HIPAA ("OZP"). In de volledige tekst van de OZP, te raadplegen op http://aka.ms/BAA, worden de Online Diensten of Professionele Diensten vermeld waarop de OZP van toepassing is. De Klant kan ervoor kiezen de OZP niet van toepassing te verklaren door de volgende informatie middels een schriftelijke kennisgeving aan Microsoft te sturen (overeenkomstig de voorwaarden van de overeenkomst van de Klant):

- de volledige wettelijke naam van de Klant en elke gelieerde Onderneming waarop deze bepalingen niet van toepassing worden verklaard; en
- als de Klant meerdere overeenkomsten heeft, de overeenkomst van de Klant waarop deze bepalingen niet meer van toepassing zijn.

Telecommunicatiegegevens

Voor zover Microsoft verkeer, inhoud en andere Persoonsgegevens verwerkt bij het leveren van Producten en Diensten die onder toepasselijk recht gelden als telecommunicatiediensten, kunnen specifieke wettelijke verplichtingen van toepassing zijn. Microsoft houdt zich aan alle wetten en voorschriften met betrekking tot telecommunicatie die van toepassing zijn op de levering van de Producten en Diensten, met inbegrip van het melden van een inbreuk op de beveiliging, de Vereisten voor Bescherming van Persoonsgegevens en de geheimhouding van telecommunicatie. De Klant is

verantwoordelijk voor het verkrijgen van de benodigde toestemming van de eindgebruikers in verband met het gebruik van Producten en Diensten die kwalificeren als telecommunicatiediensten.

California Consumer Privacy Act (CCPA)

Indien Microsoft de Persoonsgegevens verwerkt binnen de draagwijdte van de CCPA, neemt Microsoft de volgende aanvullende verplichtingen op zich jegens te Klant. Microsoft verwerkt Klantgegevens, Gegevens van Professionele Diensten en Persoonsgegevens namens de Klant en bewaart, gebruikt of verstrekt deze gegevens niet voor enig ander doel dan voor de doeleinden die worden beschreven in de Voorwaarden van de BBP en zoals is toegestaan op grond van de CCPA, met inbegrip van enige "verkoop"-uitzondering. In geen geval zal Microsoft dergelijke gegevens verkopen. Deze CCPA-voorwaarden vormen geen beperking of vermindering van de verplichtingen met betrekking tot de bescherming van persoonsgegevens die Microsoft op zich neemt in de Voorwaarden van de BBP, Productvoorwaarden of een andere overeenkomst tussen Microsoft en de Klant.

Biometrische Gegevens

Indien de Klant gebruikmaakt van Producten en Diensten voor het verwerken van Biometrische Gegevens, is de Klant verantwoordelijk voor: (i) het in kennis stellen van betrokkenen, onder andere met betrekking tot bewaarperioden en vernietiging; (ii) het verkrijgen van toestemming van betrokkenen; en (iii) het verwijderen van de Biometrische Gegevens, zoals gepast en vereist is op grond van de toepasselijke Vereisten voor Bescherming van Persoonsgegevens. Microsoft verwerkt de Biometrische Gegevens volgens de gedocumenteerde instructies van de Klant (zoals beschreven in het bovenstaande artikel "Rollen en verantwoordelijkheden van de verwerker en de verwerkingsverantwoordelijke") en beschermt deze Biometrische Gegevens overeenkomstig de voorwaarden voor gegevensbeveiliging en -bescherming van deze BBP. Binnen de context van dit artikel heeft "Biometrische Gegevens" de betekenis die wordt beschreven in Artikel 4 van de AVG en, indien van toepassing, equivalente bepalingen in andere Vereisten voor Bescherming van Persoonsgegevens.

Aanvullende Professionele Diensten.

In de onderstaande artikelen heeft de gedefinieerde term "Professionele Diensten" ook betrekking op Aanvullende Professionele Diensten en heeft de gedefinieerde term "Gegevens van Professionele Diensten" ook betrekking op gegevens die zijn verkregen voor Aanvullende Professionele Diensten.

Voor Aanvullende Professionele Diensten zijn de volgende artikelen van de BBP op dezelfde wijze van toepassing als op Professionele Diensten: "Inleiding", "Naleving van wetten", "Aard van de verwerking; eigendom", "Bekendmaking van verwerkte gegevens", "Verwerking van persoonsgegevens; AVG", de eerste paragraaf van "Beveiligingsmaatregelen en -beleid", "Verantwoordelijkheden van de Klant", "Kennisgeving van Beveiligingsincidenten", "Gegevensoverdracht" (met inbegrip van de bepalingen betreffende de Modelcontractbepalingen van 2021), de derde paragraaf van "Bewaring en verwijdering van gegevens", "Geheimhoudingsplicht van de verwerker", "Kennisgeving en maatregelen betreffende het gebruik van Subverwerkers", "Zakenpartner HIPAA" (voor zover van toepassing in de OZP), "California Consumer Privacy Act (CCPA)", "Biometrische Gegevens", "Contact opnemen met Microsoft", "Bijlage B – Betrokkenen en categorieën van persoonsgegevens" en "Bijlage C – Bijlage voor aanvullende waarborgen".

Contact opnemen met Microsoft

Als de Klant van mening is dat Microsoft zich niet houdt aan haar privacy- of beveiligingsverplichtingen, kan de Klant contact opnemen met de klantondersteuning of het Privacy-webformulier van Microsoft gebruiken dat te vinden is op http://go.microsoft.com/?linkid=9846224. Het postadres van Microsoft is:

Microsoft Enterprise Service Privacy.
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052 USA

Microsoft Ireland Operations Limited is de vertegenwoordiger van Microsoft voor gegevensbescherming voor de Europese Economische Ruimte en Zwitserland. De vertegenwoordiger voor privacy van Microsoft Ireland Operations Limited is te bereiken op het volgende adres.

Microsoft Ireland Operations, Ltd.
Attn: Data Protection
One Microsoft Place
South County Business Park
Leopardstown
Dublin 18, D18 P521, Ireland

Bijlage A – Beveiligingsmaatregelen

Microsoft heeft voor Klantgegevens in de Core Online Diensten en Gegevens van Professionele Diensten de volgende beveiligingsmaatregelen geïmplementeerd en zal deze onderhouden. Dit, samen met de beveiligingsverplichtingen in deze BBP (met inbegrip van de AVG-voorwaarden), is de enige verantwoordelijkheid van Microsoft met betrekking tot de beveiliging van deze gegevens.

Domein	Praktijken
Organisatie van gegevensbeveiliging	**Eigendom van beveiliging.** Microsoft heeft een of meer beveiligingsfunctionarissen aangewezen die verantwoordelijk zijn voor het coördineren en controleren van de beveiligingsregels en -procedures. **Beveiligingsrollen en -verantwoordelijkheden.** Medewerkers van Microsoft met toegang tot Klantgegevens of Gegevens van Professionele Diensten zijn onderworpen aan verplichtingen met betrekking tot vertrouwelijkheid. **Programma voor risicobeheer.** Microsoft heeft een risicobeoordeling uitgevoerd voordat de Klantgegevens worden verwerkt of de Online Dienst wordt gestart, en voordat de Gegevens van Professionele Diensten worden verwerkt of de Professionele Diensten worden gestart. Microsoft bewaart de beveiligingsdocumenten nadat de geldigheid ervan is verstreken conform haar bewaartermijnvereisten.
Beheer van bedrijfsmiddelen	**Inventaris van bedrijfsmiddelen.** Microsoft houdt een inventaris bij van alle media waarop Klantgegevens of Gegevens van Professionele Diensten zijn opgeslagen. Toegang tot de inventarissen van die media is beperkt tot medewerkers van Microsoft die daar schriftelijke toestemming voor hebben. **Behandeling van bedrijfsmiddelen** • Microsoft classificeert Klantgegevens of Gegevens van Professionele Diensten om deze herkenbaar te maken en om toegang daartoe in gepaste mate te beperken. • Microsoft legt beperkingen op met betrekking tot het afdrukken van Klantgegevens en Gegevens van Professionele Diensten en beschikt over procedures voor het vernietigen van afgedrukt materiaal dat dergelijke gegevens bevat.

Domein	Praktijken
	• Medewerkers van Microsoft moeten toestemming van Microsoft verkrijgen voorafgaande aan het opslaan van Klantgegevens of Gegevens van Professionele Diensten op draagbare apparaten, het op afstand raadplegen van dergelijke gegevens of het verwerken van dergelijke gegevens buiten de faciliteiten van Microsoft.
Beveiliging van personeelszaken	**Beveiligingstraining.** Microsoft stelt haar medewerkers op de hoogte van relevante beveiligingsprocedures en hun rol daarbij. Microsoft stelt haar medewerkers ook op de hoogte van de mogelijke gevolgen van het schenden van de beveiligingsregels en -procedures. Microsoft gebruikt alleen anonieme gegevens bij de training.
Fysieke en omgevingsbeveiliging	**Fysieke toegang tot faciliteiten.** Microsoft beperkt de toegang tot faciliteiten waar informatiesystemen zijn geplaatst waarmee Klantgegevens of Gegevens van Professionele Diensten worden verwerkt, tot geïdentificeerde, geautoriseerde personen. **Fysieke toegang tot componenten.** Microsoft houdt een bestand bij van binnenkomende en uitgaande media die Klantgegevens of Gegevens van Professionele Diensten bevatten, waaronder het type media, de geautoriseerde afzender/ontvangers, de datum en het tijdstip, het aantal media en de typen van dergelijke gegevens die deze bevatten. **Bescherming tegen verstoringen.** Microsoft gebruikt verschillende systemen die voldoen aan industrienormen om te beschermen tegen gegevensverlies vanwege stroom- of lijnstoringen. **Verwijdering van onderdelen.** Microsoft maakt gebruik van procedures die aan industrienormen voldoen, om Klantgegevens en Gegevens van Professionele Diensten te verwijderen wanneer deze niet langer nodig zijn.
Beheer van communicatie en operationele activiteiten	**Operationeel beleid.** Microsoft houdt beveiligingsdocumenten bij met beschrijvingen van de beveiligingsmaatregelen en de relevante procedures en verantwoordelijkheden van haar medewerkers die toegang hebben tot Klantgegevens en Gegevens van Professionele Diensten. **Procedures voor gegevensherstel** • Microsoft beheert voortdurend, maar in ieder geval niet minder vaak dan eens per week (tenzij er tijdens die periode geen gegevens zijn bijgewerkt) meerdere exemplaren van de Klantgegevens en Gegevens

Domein	Praktijken
	van Professionele Diensten waarmee dergelijke gegevens kunnen worden hersteld. • Microsoft slaat exemplaren van de Klantgegevens en Gegevens van Professionele Diensten en herstelprocedures op een andere locatie op dan de locatie van de primaire computerapparatuur waarmee de Klantgegevens en Gegevens van Professionele Diensten worden verwerkt. • Microsoft heeft specifieke procedures geïmplementeerd waarmee de toegang tot Klantgegevens en Gegevens van Professionele Diensten wordt beheerd. • Microsoft evalueert de procedures voor gegevensherstel ten minste eenmaal per zes maanden, uitgezonderd de gegevensherstelprocedures voor Professionele Diensten en voor Azure Government Services, die elke twaalf maanden worden geëvalueerd. • Microsoft houdt een logboek bij van de pogingen tot gegevensherstel, waaronder de verantwoordelijke persoon, de beschrijving van de herstelde gegevens en indien van toepassing, de persoon die daarvoor verantwoordelijk is, en welke gegevens eventueel handmatig moesten worden ingevoerd tijdens het gegevensherstel. **Schadelijke software.** Microsoft beschikt over programma's die voorkomen dat met behulp van schadelijke software ongeoorloofde toegang wordt verschaft tot Klantgegevens en Gegevens van Professionele Diensten, waaronder schadelijke software afkomstig uit openbare netwerken. **Gegevens buiten grenzen** • Microsoft versleutelt Klantgegevens en Gegevens van Professionele Diensten die worden overgedragen via openbare netwerken, of stelt de Klant in staat dat te doen. • Microsoft beperkt de toegang tot Klantgegevens en Gegevens van Professionele Diensten op media die buiten de faciliteiten worden overgebracht. **Registratie van gebeurtenissen.** Microsoft registreert toegang tot en gebruik van informatiesystemen die Klantgegevens of Gegevens van Professionele Diensten bevatten, of stelt de Klant in staat dit te doen.

Domein	Praktijken
	Hierbij wordt de toegangs-id, tijd, verleende of geweigerde autorisatie en relevante activiteit vastgelegd.
Toegangsbeheer	**Toegangsbeleid.** Microsoft houdt een bestand bij met beveiligingsmachtigingen van personen die toegang hebben tot Klantgegevens of Gegevens van Professionele Diensten. **Machtiging tot toegang** • Microsoft houdt een bestand bij met medewerkers die zijn gemachtigd tot toegang tot Microsoft-systemen die Klantgegevens of Gegevens van Professionele Diensten bevatten. • Microsoft schakelt authenticatiereferenties die gedurende een periode van niet langer dan zes maanden niet zijn gebruikt, uit. • Microsoft identificeert de medewerkers die geoorloofde toegang tot gegevens en resources verlenen, wijzigen of intrekken. • Microsoft zorgt ervoor dat, waar meer dan één persoon toegang heeft tot systemen met Klantgegevens of Gegevens van Professionele Diensten, elke persoon een eigen identifier/aanmeldingsnaam heeft. **Minimale rechten** • Technisch ondersteunend personeel heeft alleen toegang tot Klantgegevens of Gegevens van Professionele Diensten indien nodig. • Microsoft beperkt toegang tot Klantgegevens of Gegevens van Professionele Diensten tot die personen voor wie toegang tot Klantgegevens nodig is om hun werk te kunnen uitvoeren. **Integriteit en vertrouwelijkheid** • Microsoft draagt medewerkers van Microsoft op beheersessies af te sluiten bij het verlaten van locaties die in het beheer van Microsoft zijn, of wanneer computers anderszins onbeheerd zijn. • Microsoft slaat wachtwoorden zodanig op dat ze onbegrijpelijk zijn wanneer ze in gebruik zijn. **Authenticatie** • Microsoft gebruikt praktijken die voldoen aan branchenormen om gebruikers die proberen zich toegang te verschaffen tot gegevenssystemen, te identificeren en te verifiëren.

Domein	Praktijken
	• Waar authenticatiemechanismen gebaseerd zijn op wachtwoorden, vereist Microsoft dat de wachtwoorden regelmatig worden vernieuwd. • Waar authenticatiemechanismen gebaseerd zijn op wachtwoorden, vereist Microsoft dat de wachtwoorden ten minste acht tekens lang zijn. • Microsoft zorgt ervoor dat uitgeschakelde of verlopen id's niet aan andere personen worden verleend. • Microsoft houdt toezicht op herhaalde pogingen tot het openen van de gegevenssystemen met een ongeldig wachtwoord, of stelt de Klant in staat hierop toezicht te houden. • Microsoft maakt gebruik van procedures die voldoen aan industrienormen, om wachtwoorden die zijn beschadigd of per ongeluk onthuld, uit te schakelen. • Microsoft gebruikt voor het beschermen van wachtwoorden procedures die voldoen aan industrienormen, waaronder procedures voor het behouden van de vertrouwelijkheid en integriteit van wachtwoorden, bij het toewijzen, verspreiden en opslaan van wachtwoorden. **Netwerkontwerp.** Microsoft beschikt over middelen om te voorkomen dat personen die zich toegangsrechten toe-eigenen die niet aan hen zijn toegewezen, toegang verkrijgen tot Klantgegevens of Gegevens van Professionele Diensten waartoe zij niet zijn gemachtigd.
Beheer van incidenten gegevensbeveiliging	**Antwoordprocedure incidenten** • Microsoft houdt een bestand bij met schendingen van de beveiliging, met een beschrijving van de schending, de periode en de gevolgen van de schending, de naam van degene die de schending meldt, de naam van degene aan wie de schending wordt gemeld, en de procedure voor het herstellen van gegevens. • Voor elke schending van de beveiliging die een Beveiligingsincident inhoudt, wordt door Microsoft zonder onnodige vertraging, en in elk geval binnen 72 uur, een kennisgeving verstrekt (zoals beschreven in de sectie “Kennisgeving van Beveiligingsincidenten” hierboven). • Microsoft houdt de openbaarmaking van Klantgegevens of Gegevens van Professionele Diensten bij, met inbegrip van welke gegevens openbaar zijn gemaakt, aan wie en op welke tijdstippen, of stelt de Klant in staat dat te doen.

Domein	Praktijken
	Service Monitoring. Beveiligingsmedewerkers van Microsoft controleren logboeken ten minste elke zes maanden om indien noodzakelijk herstelprocedures voor te stellen.
Beheer bedrijfscontinuïteit	• Microsoft beschikt over nood- en calamiteitenplannen voor de faciliteiten waar de informatiesystemen van Microsoft zijn geplaatst waarmee Klantgegevens of Gegevens van Professionele Diensten worden verwerkt. • De redundante opslag en de procedures voor gegevensherstel van Microsoft zijn ontworpen om de Klantgegevens of Gegevens van Professionele Diensten te kunnen herstellen in de originele of laatst gerepliceerde staat voordat de gegevens verloren raakten of vernietigd werden.

Bijlage B – Betrokkenen en categorieën van persoonsgegevens

Betrokkenen: Tot de betrokkenen behoren de vertegenwoordigers en eindgebruikers van de Klant met inbegrip van werknemers, opdrachtnemers en klanten van de Klant. Tot de betrokkenen behoren mogelijk tevens individuele personen die trachten te communiceren met of persoonlijke informatie over te dragen aan gebruikers van de diensten die worden geleverd door Microsoft. Microsoft erkent dat, afhankelijk van het gebruik van de Producten en Diensten door de Klant, de Klant ervoor kan kiezen persoonsgegevens van een of meer van de onderstaande typen van betrokkenen in de persoonsgegevens op te nemen:

- medewerkers, opdrachtnemers, tijdelijke krachten (huidige, voormalige, toekomstige) van de Klant;
- inwonenden van bovenstaande;
- Zakelijk partners/contactpersonen van de Klant (natuurlijke personen) of medewerkers, opdrachtnemers of tijdelijke krachten van zakelijk partners/contactpersonen (rechtspersoon) (huidige, voormalige, toekomstige);

- gebruikers (bijvoorbeeld klanten, cliënten, patiënten, bezoekers, enz.) en andere betrokkenen die gebruikers zijn van de diensten van de Klant;
- Zakelijk in partners, belanghebbenden of personen die actief samenwerken, communiceren of op andere wijzen contact hebben met medewerkers van de Klant en/of gebruikmaken van communicatiehulpmiddelen als door de Klant aangeleverde apps en websites;
- belanghebbenden of personen die passief contact hebben met de Klant (bijvoorbeeld omdat ze het onderwerp zijn van een onderzoek of worden vermeld in documenten of van correspondentie met de Klant);
- minderjarigen; of
- Beroepsbeoefenaren met beroepsgeheim (bijvoorbeeld artsen, advocaten, notarissen, religieuze beambten, enzovoort).

Categorieën gegevens: De persoonsgegevens die zijn opgenomen in e-mail, documenten en andere gegevens in elektronische vorm in de context van de Producten en Diensten. Microsoft erkent dat, afhankelijk van het gebruik van de Producten en Diensten door de Klant, de Klant ervoor kan kiezen persoonsgegevens van een of meer van de onderstaande categorieën in de persoonsgegevens op te nemen:

- basispersoonsgegevens (bijvoorbeeld geboorteplaats, straatnaam en huisnummer (adres), postcode, woonplaats, woonland, mobiele telefoonnummer, voornaam, achternaam, voorletters, e-mailadres, geslacht, geboortedatum), met inbegrip van basispersoonsgegevens over familieleden en kinderen;
- verificatiegegevens (bijvoorbeeld gebruikersnaam, wachtwoord of pincode, beveiligingsvraag, controlespoor);
- contactgegevens (bijvoorbeeld adressen, e-mailadres, telefoonnummers, socialemedia-id's; noodcontactgegevens);
- unieke identificatienummers en handtekeningen (bijvoorbeeld burgerservicenummer, bankrekeningnummer, paspoort- en identiteitsbewijsnummer, rijbewijsnummer en voertuigregistratiegegevens, IP-adressen, personeelsnummer, studentennummer, patiëntennummer, handtekening, unieke identifier in tracking cookies of vergelijkbare technologie);
- pseudonieme identifiers;
- financiële en verzekeringsgegevens (bijvoorbeeld polisnummer, naam en nummer van bankrekening, naam en nummer van creditcard, factuurnummer, inkomen, type verzekering, betaalgedrag, kredietwaardigheid);

- commerciële gegevens (bijvoorbeeld aankoopgeschiedenis, speciale aanbiedingen, abonnementsgegevens, betaalgeschiedenis);
- biometrische gegevens (bijvoorbeeld dna, vingerafdrukken en irisscans);
- locatiegegevens (bijvoorbeeld gsm-id, geolocatienetwerkgegevens, locatie op het moment van het begin/eind van het gesprek, locatiegegevens afgeleid van het gebruik van Wi-Fi-toegangspunten);
- foto's, video en audio;
- internetactiviteit (bijvoorbeeld browsegeschiedenis, zoekgeschiedenis, activiteiten als lezen, televisie kijken en radio luisteren);
- apparaat-id (bijvoorbeeld IMEI-nummer, simkaartnummer, MAC-adres);
- profilering (bijvoorbeeld op basis van waargenomen crimineel of asociaal gedrag, of pseudonieme profielen op basis van bezochte URL's, clickstreams, browselogboeken, IP-adressen, domeinen, geïnstalleerde apps, of profielen op basis van marketingvoorkeuren);
- gegevens van personeelszaken en werving (bijvoorbeeld verklaring van dienstverband, wervingsgegevens (zoals curriculum vitae, werkgeschiedenis, opleidingsgeschiedenis), functie- en positiegegevens, met inbegrip van gewerkte uren, beoordelingen en salaris, werkvergunninggegevens, beschikbaarheid. arbeidsvoorwaarden, fiscale gegevens, betalingsgegevens, verzekeringsgegevens en locatie en organisaties);
- opleidingsgegevens (bijvoorbeeld opleidingsgeschiedenis, huidig opleidingsniveau, cijfers en resultaten, hoogst genoten opleiding, leerbeperkingen);
- informatie over staatsburgerschap en verblijfsgegevens (bijvoorbeeld staatsburgerschap, naturalisatiestatus, burgerlijke staat, nationaliteit, immigratiestatus, paspoortgegevens, verblijfs- of werkvergunning);
- informatie verwerkt voor het uitvoeren van een taak uitgevoerd in het openbaar belang of in het kader van de uitoefening van een officiële bevoegdheid;
- speciale categorieën van gegevens (bijvoorbeeld ras of etnische oorsprong, politieke mening, religieuze of filosofische overtuiging, vakbondslidmaatschap, genetische gegevens, biometrische gegevens voor de unieke identificatie van een natuurlijke persoon, gezondheidsgegevens, gegevens over het seksleven of de seksuele geaardheid van een natuurlijke persoon, of gegevens met betrekking tot strafrechtelijke veroordelingen of overtredingen); of
- andere persoonsgegevens vermeld in artikel 4 van de AVG.

Bijlage C – Bijlage voor aanvullende waarborgen

Door middel van deze Bijlage voor aanvullende waarborgen bij de BBP (deze "Bijlage") biedt Microsoft aanvullende waarborgen aan de Klant met betrekking de verwerking van persoonsgegevens, binnen de reikwijdte van de AVG, door Microsoft namens de Klant, en aanvullende verhaalsmogelijkheden voor de betrokkenen op wie de persoonsgegevens betrekking hebben.

Deze Bijlage is een aanvulling op en onderdeel van, maar geen variant of wijziging van, de BBP.

1. **Aanvechting van bevelen.** In het geval dat Microsoft een bevel ontvangt van een derde partij voor gedwongen bekendmaking van persoonsgegevens die zijn verwerkt op grond van deze BBP, zal Microsoft:
    a. al het redelijkerwijs mogelijke doen om de derde partij door te wijzen om de gegevens rechtstreeks bij de Klant op te vragen;
    b. de Klant onverwijld op de hoogte stellen, tenzij dit verboden is krachtens de wetgeving van de verzoekende derde partij en, indien het verboden is om de Klant op de hoogte te stellen, al het wettelijk mogelijke doen om het verbod op te heffen om zo snel mogelijk zoveel mogelijk informatie aan de Klant te verstrekken; en
    c. al het wettelijk mogelijke doen om het bevel voor bekendmaking aan te vechten op grond van juridische tekortkomingen in de wetgeving van de verzoekende partij of op grond van relevante tegenstrijdigheden met het toepasselijk recht van de Europese Unie of de wetgeving van de toepasselijke Lidstaat.

Indien Microsoft of een van haar gelieerde ondernemingen na het nemen van de stappen beschreven in a. tot en met c. hierboven nog steeds genoodzaakt is om persoonsgegevens bekend te maken, maakt Microsoft uitsluitend de minimale hoeveelheid van die gegevens bekend die noodzakelijk is om te voldoen aan het bevel tot gedwongen bekendmaking.

Voor de doeleinden van deze bepaling omvat al het wettelijk mogelijke geen acties die resulteren in burgerlijke en strafrechtelijke sancties zoals minachting van het hof onder het recht van de desbetreffende jurisdictie.

2. **Vrijwaring van betrokkenen.** Met inachtneming van Artikelen 3 en 4 zal Microsoft een betrokkene vergoeden van materiële of immateriële schade voor de betrokkene die is veroorzaakt door de bekendmaking door Microsoft van Persoonsgegevens van de betrokkene die zijn overgedragen naar aanleiding van een bevel van een overheidsinstelling

of wetshandhavingsinstantie buiten de EU/EER in strijd met de verplichtingen van Microsoft op grond van Hoofdstuk V van de AVG (een "Relevante Bekendmaking"). Niettegenstaande het voorgaande, is Microsoft niet verplicht om de betrokkene krachtens Artikel 2 te vergoeden indien de betrokkenen reeds een vergoeding heeft ontvangen voor dezelfde schade, ongeacht of deze vergoeding afkomstig is van Microsoft of een andere partij.

3. **Voorwaarden voor Vrijwaring.** Vrijwaring krachtens artikel 2 is ervan afhankelijk of de betrokkenen, naar redelijke tevredenheid van Microsoft, kan vaststellen dat:
   a. Microsoft heeft een Relevante Bekendmaking verricht;
   b. de Relevante Bekendmaking was de grondslag voor een officiële procedure die door de overheidsinstelling of wetshandhavingsinstantie buiten de EU/EER is aangespannen tegen de betrokkenen; en
   c. de Relevante Bekendmaking was de directe oorzaak van de materiële of niet-materiële schade die de betrokkene heeft geleden.

De bewijslast ten aanzien van de voorwaarden a. tot en met c. rust op de betrokkene.

Niettegenstaande het voorgaande, is Microsoft niet verplicht om de betrokkene krachtens Artikel 2 te vrijwaren indien Microsoft vaststelt dat de Relevante Bekendmaking niet in strijd was met de in hoofdstuk V van de AVG vastgestelde voorwaarden.

4. **Omvang van de schade.** Vrijwaring krachtens artikel 2 is beperkt tot materiële of niet-materiële schade zoals uiteengezet in de AVG en sluit gevolgschade en andere schade uit die niet het gevolg is van schending van de AVG door Microsoft.

5. **Uitoefening van rechten.** De rechten die krachtens dit Aanhangsel worden verleend aan betrokkenen, kunnen door de betrokkene worden afgedwongen bij Microsoft ongeacht enige beperking in Bepaling 2 of 6 van de Modelcontractbepalingen. De betrokkenen kan alleen een vordering op grond van dit Aanhangsel instellen op individuele basis en niet als onderdeel van een groepsvordering of collectieve of representatieve actie. De rechten die krachtens dit Aanhangsel worden verleend aan betrokkenen zijn persoonlijk aan de betrokkenen verbonden en mogen niet worden overgedragen.

6. **Kennisgeving van wijzigingen.** Microsoft stemt ermee in en garandeert geen reden te hebben om aan te nemen dat de wetgeving die van toepassing is op haar of haar subverwerkers, inclusief in iederland waarnaar persoonsgegevens hetzij door haarzelf, hetzij via een subverwerker worden doorgegeven, haar belet de van deKlant ontvangen instructies en haar verplichtingen krachtens dit Aanhangsel of de Modelcontractbepalingen van 2021 na te komen, en dat zij, in geval van een wijziging in deze wetgeving die naar verwachting een aanzienlijk nadelig effect zal hebben op de door dit Aanhangsel of de Modelcontractbepalingen geboden

garanties en verplichtingen, de Klant onverwijld in kennis zal stellen van de wijziging zodra zij daarvan op de hoogte is, in welk geval de Klant gerechtigd is de doorgifte van gegevens op te schorten en/of het contract te beëindigen.

Bijlage D – Bezwaren tegen een bevel of bindende wettelijke verplichting tot opschorting van Online Diensten

Met deze bijlage doet Microsoft de volgende toezeggingen aan nationale, federale en regionale overheidsklanten van de lidstaten van de Europese Unie ("EU"), evenals de EU-toetredingslanden, leden van de Europese Vrijhandelsassociatie, het Verenigd Koninkrijk, Monaco, Vaticaanstad en de Europese Commissie ("Beschermde overheidsklant").

1. Indien Microsoft een bevel ontvangt of anderszins onderworpen is aan een bindende wettelijke verplichting van een overheid, agentschap, commissie of quasi-overheidsorgaan dat Microsoft verplicht om de levering, geheel of gedeeltelijk, van Online Diensten (inclusief, maar niet beperkt tot, de levering van Microsoft Azure Diensten, Microsoft Dynamics 365 Diensten of Office 365 Diensten) aan de Beschermde Overheidsklant op te schorten of te staken, zal Microsoft, namens zichzelf en haar Gelieerde Ondernemingen:
    a. de beschikbare middelen gebruiken om de vrijwillige intrekking, herroeping of vernietiging van een dergelijke order te bewerkstelligen; en
    b. alle rechtmatige inspanningen verrichten om het bevel aan te vechten bij de rechtbanken van het land waarvan de regering het bevel heeft uitgevaardigd op basis van eventuele wettelijke tekortkomingen in de wetgeving van de bestellende partij of eventuele relevante conflicten met het toepasselijke recht van de Europese Unie of het toepasselijke recht van de hierboven genoemde landen.

    Microsoft zal indien nodig een permanent en voorlopig gerechtelijk bevel aanvragen om de continue en ononderbroken levering van de relevante Online Diensten te waarborgen, totdat de volledige en definitieve uitspraak is gedaan over rechtmatige pogingen om het bevel of andere bindende wettelijke verplichting waarnaar hierboven wordt verwezen, aan te vechten.
2. Rechten die op grond van deze bepaling aan de Klant worden verleend, zijn persoonlijk voor de Beschermde Overheidsklant en mogen niet worden overgedragen.

Bijlage 1 – Voorwaarden van de Algemene Verordening Gegevensbescherming van de Europese Unie

Microsoft verbindt zich aan deze AVG-voorwaarden voor alle klanten met ingang van 25 mei 2018. Deze verplichtingen zijn bindend voor Microsoft jegens de Klant, ongeacht (1) de versie van de Productvoorwaarden en BBP die overigens van toepassing zijn op een gegeven Productabonnement of -licentie, of (2) enig andere overeenkomst waarin wordt verwezen naar deze bijlage.

In het kader van deze AVG-voorwaarden komen de Klant en Microsoft overeen dat de Klant de verwerkingsverantwoordelijke en Microsoft de verwerker is met betrekking tot de Persoonsgegevens, uitgezonderd in gevallen dat de Klant optreedt als verwerker van de Persoonsgegevens. In dat geval is Microsoft een subverwerker. Deze AVG-voorwaarden zijn van toepassing op de verwerking van Persoonsgegevens namens de Klant door Microsoft binnen de reikwijdte van de AVG. Deze AVG-voorwaarden vormen geen beperking of vermindering van de verplichtingen met betrekking tot de bescherming van persoonsgegevens die Microsoft op zich neemt in de Productvoorwaarden of enig andere overeenkomst tussen Microsoft en de Klant. Deze AVG-voorwaarden zijn niet van toepassing wanneer Microsoft de Verwerkingsverantwoordelijke is met betrekking tot Persoonsgegevens.

Relevante AVG-verplichtingen: Artikelen 5, 28, 32 en 33

1. Microsoft ondersteunt de verantwoordingsverplichtingen van de Klant via deze BBP en de productdocumentatie die aan de Klant wordt verstrekt, en blijft dit doen gedurende de looptijd van het abonnement van de Klant of de toepasselijke overeenkomst voor de levering van Professionele Diensten, in het kader van artikellid 3(h) hieronder. (Artikel 5(2))
2. Microsoft neemt geen andere verwerker in dienst zonder voorafgaande specifieke of algemene schriftelijke toestemming van de Klant. In het geval van algemene schriftelijke toestemming licht Microsoft de Klant in over beoogde veranderingen inzake de toevoeging of vervanging van andere verwerkers, waarbij de Klant de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken. (Artikel 28, lid 2)
3. De verwerking door Microsoft wordt geregeld door deze AVG-voorwaarden krachtens het recht van de Europese Unie of de lidstaat (hierna “Unierecht of het lidstatelijk recht”) die de

Microsoft ten aanzien van de Klant bindt. Het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort Persoonsgegevens en de categorieën van betrokkenen, en de rechten en verplichtingen van de Klant worden omschreven in de licentieovereenkomst van de Klant, waarin deze AVG-voorwaarden zijn opgenomen. Hierin is met name bepaalt dat Microsoft:

a. de Persoonsgegevens uitsluitend verwerkt op basis van schriftelijke instructies van de Klant, onder meer met betrekkingtot doorgiften van Persoonsgegevens aan een derde land of een internationale organisatie, tenzij een op Microsoft van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling Microsoft tot verwerking verplicht; in dat geval stelt Microsoft de Klant, voorafgaand aan de verwerking, in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt;
b. waarborgt dat de tot het verwerken van de Persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden;
c. alle overeenkomstig artikel 32 van de AVG vereiste maatregelen neemt;
d. aan de in de leden 2 en 4 bedoelde voorwaarden voor het in dienst nemen van een andere verwerker voldoet;
e. rekening houdend met de aard van de verwerking, de Klant door middel van passende technische en organisatorische maatregelen, voor zover mogelijk, bijstand verleent bij het vervullen van de plicht van de Klant om verzoeken om uitoefening van de in hoofdstuk III van de AVG vastgestelde rechten van de betrokkene te beantwoorden;
f. rekening houdend met de aard van de verwerking en de Microsoft ter beschikking staande informatie de Klant bijstand verleent bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de AVG;
g. na afloop van de verwerkingsdiensten, naargelang de keuze van de Klant, alle Persoonsgegevens wist of deze aan de Klant terugbezorgt, en bestaande kopieën verwijdert, tenzij opslag van de Persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht;
h. de Klant alle informatie ter beschikking stelt die nodig is om de nakoming van de in artikel 28 van de AVG genoemde verplichtingen aan te tonen en audits, waaronder inspecties, door de Klant of een door de Klant gemachtigde controleur mogelijk te maken en eraan bij te dragen.

Microsoft zal de Klant onmiddellijk informeren indien een instructie, naar mening van Microsoft, in strijd is met de AVG of andere Unierechtelijke of lidstaatrechtelijke bepalingen wat betreft de bescherming van persoonsgegevens. (Artikel 28, lid 3)

4. Wanneer Microsoft een andere verwerker in dienst neemt om bepaalde verwerkingsactiviteiten voor de Klant te verrichten, worden dezelfde verplichtingen wat

betreft de bescherming van persoonsgegevens die in deze AVG-voorwaarden zijn uiteengezet, opgelegd aan deze andere verwerker door middel van een overeenkomst of een andere rechtshandeling op grond van het Unierecht of lidstatelijk recht. Dit geldt in het bijzonder om voldoende garanties te bieden om passende technische en organisatorische maatregelen uit te voeren zodat de verwerking voldoet aan de voorwaarden van de AVG. Wanneer de andere verwerker zijn verplichtingen inzake gegevensbescherming niet nakomt, blijft Microsoft ten aanzien van de Klant volledig aansprakelijk voor het nakomen van de verplichtingen van die andere verwerker. (Artikel 28, lid 4)

5. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de Klant en Microsoft passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:
   a. de pseudonimisering en versleuteling van Persoonsgegevens;
   b. het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
   c. het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de Persoonsgegevens tijdig te herstellen; en
   d. een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen om de veiligheid van de verwerking te garanderen. (Artikel 32, lid 1)
6. Bij de beoordeling van het passende beveiligingsniveau wordt rekening gehouden met de risico's die ontstaan door verwerking, vooral als gevolg van de vernietiging, het verlies, de wijziging, de ongeoorloofde bekendmaking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte Persoonsgegevens, hetzij per ongeluk hetzij onrechtmatig. (Artikel 32, lid 2)
7. De Klant en Microsoft treffen maatregelen om ervoor te zorgen dat iedere natuurlijke persoon die handelt onder het gezag van de Klant of van Microsoft en toegang heeft tot Persoonsgegevens, deze slechts in opdracht van de Klant verwerkt, tenzij hij of zij daartoe Unierechtelijk of lidstaatrechtelijk toe verplicht is. (Artikel 32, lid 4)
8. Microsoft informeert de Klant zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met Persoonsgegevens. (Artikel 33, lid 2). In een dergelijke kennisgeving dient de informatie te zijn opgenomen die een verwerker verplicht is te

verstrekken aan een verwerkingsverantwoordelijke op grond van artikel 33, lid 3, voor zover deze informatie redelijkerwijs beschikbaar is voor Microsoft.