

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Als gemeente zijn we verplicht een DPIA uit te voeren als er sprake is van een verhoogd risico op een inbreuk op de persoonlijke levenssfeer van onze inwoners. De DPIA vul je aan het begin van je project in. Hierdoor kunnen maatregelen voor het beschermen van data en het voorkomen van risico's vooraf meegenomen worden in de afweging om tot de verwerking over te gaan of waar mogelijk meegenomen worden in het ontwerp op programma van eisen van de aan te schaffen applicatie.

De DPIA vul je samen met je I-adviseur in. De DPIA is onderdeel van de intakeprocedure van het afstemmingsoverleg.

Project	: Microsoft 365
Afdeling	: Personeel, Informatie, Facilitair
Verantwoordelijk	: 5.1.2e
I-adviseur	: 5.1.2e
Datum	: 28-7-2024

1. Inleiding op het project

1.1 Wat zijn de algemene achtergronden van het project?

Microsoft 365 is een cloudproductiviteitsplatform. Met de verschillende toepassingen binnen Microsoft 365 (ook wel MS365) kunnen een reeks aan taken uitgevoerd worden. Het heeft als hoofdfunctie om samenwerkingsmogelijkheden en informatievastlegging te verbeteren. Centraal staan hierin Teams en Sharepoint. Dit is de volgende stap in de ontwikkeling van kantoorautomatisering.

Voor werk waarbij proceslogistiek (continu op tijd leveren) en/of gegevens(kwaliteit) belangrijk is, zoals voor ons dienstverleningsprocessen of andere alledaagse primaire taakuitvoering, gebruiken we taakspecifieke applicaties als Allegro voor schuldhelpverlening of het generieke documentmanagementsysteem Corsa.

Uitgangspunt is dat de taken waarbij de meeste (bijzondere/gevoelige) persoonsgegevens worden verwerkt in een taakspecifieke applicatie zullen worden verricht, niet in MS365.

Op hoofdlijnen wordt MS365 gebruikt voor:

- Gereguleerd samenwerken: Uitvoeren complexe en omvangrijke projecten
- Flexibel samenwerken
 - a. Voorbereiden beleid
 - b. Uitvoeren project
 - c. Structureel overleg
 - d. Kennisdelen
- Zelfstandig werken
 - a. E-mailen
 - b. Opstellen en delen van documenten en bestanden
 - c. Agenda bijhouden
 - d. Persoonlijke planning en taken bijhouden

1.1 Welk probleem lost deze gegevensverwerking op?

In de huidige situatie maakt de gemeente gebruik van een verouderde versie van Microsoft Office die momenteel gebrekkige ondersteuning biedt. Wanneer mensen moeten samenwerken aan een bepaald document, zoals een DPIA, is er vaak sprake van meerdere verschillende versies op verschillende laptops omdat er vaker een versie van het document wordt doorgemailed in plaats van gedeeld. Dit draagt eraan bij dat de informatiehuishouding niet optimaal kan gebeuren omdat bijvoorbeeld informatie over één project verdeeld staat over mappen op 4 verschillende laptops. Hierdoor is het later ook moeilijk te achterhalen hoe besluitvorming heeft plaatsgevonden.

De gemeente Nijmegen wil MS365 gaan gebruiken om de samenwerking binnen de organisatie te verbeteren, maar ook meteen zorgen voor informatiehuishouding die hierbij passend is, die veilig is en voldoet aan wet- en regelgeving.

2. Doel en grondslag

2.1 Wat is het doel van de beoogde verwerking?

Het doel van MS365 is het bevorderen van samenwerken en niet zozeer het verwerken van persoonsgegevens. Het is echter niet uit te sluiten dat in sommige vormen van overleg persoonsgegevens worden vastgelegd, met name wanneer het voor projecten wordt gebruikt (zoals inwonersgegevens bij bouwprojecten) of structureel overleg (zoals een P&O overleg)

2.2 Op welke grondslag is de verwerking gebaseerd?

Het samenwerken binnen een digitale omgeving is gebaseerd op de grondslag *gerechtvaardigd belang*. Er is sprake van een gerechtvaardigd belang onder meer wanneer een verwerking aantoonbaar noodzakelijk is om bedrijfsactiviteiten te kunnen verrichten. MS365 is een systeem dat we gebruiken om dit te doen.

Het kan zijn dat bij een verwerking de grondslag shift naar de grondslag algemeen belang, namelijk wanneer de verwerking noodzakelijk is om de publieke taak uit te voeren – dit is wanneer een verwerking valt onder een specifieke gemeentelijke taak.

3. Achtergrond

3.1 Welke besluitvorming heeft plaatsgevonden op dit onderwerp?

In november 2020 is door de Directie en het GMT het besluit genomen om voor digitale samenwerking en kantoorautomatisering gebruik te gaan maken van het MS365-platform.

3.2 Zijn er eerder DPIA's uitgevoerd op dit onderwerp?

Er is een DPIA voor de overgang naar Exchange online uitgevoerd. Naar aanleiding van deze DPIA zijn verschillende landelijk geadviseerde maatregelen genomen. Zie hiervoor de bijlage.

Destijds is ervoor gekozen voor een andere vorm DPIA dan gebruikelijk omdat bij deze assessment de nadruk lag op de risico's en beveiligingsmaatregelen. Ook bij deze DPIA zal daar, meer dan gebruikelijk, het zwaartepunt liggen. Omdat MS365 gebruikt zal worden voor een variatie aan taken, is het namelijk lastig vooraf vast te stellen hoe de applicatie gebruikt zal worden door medewerkers, en daardoor niet uit te sluiten welke soorten persoonsgegevens erin zullen worden vastgelegd.

Maatregelen	Advies FG	Status	Toelichting
1a. eDiscovery binnen de E3 licentie gebruiken voor aanvragen mbt rechten van betrokkenen	Noodzakelijk	Niet gerealiseerd	Kan nu alleen gedaan worden door Global Admins van de IRVN. Nijmegen wil mensen binnen Nijmegen hiervoor benoemen. Probleem is dat E3 altijd tenantbreed zoekt. Opgenomen in nieuwe maatregelen-overzicht.
2a. Gebruik multifactor authenticatie	Noodzakelijk	Deels gerealiseerd	Is voor internen geregeld. Moet voor externen ingeregeld worden. Is al bekend in Topdesk . Opgenomen in nieuwe maatregelen-overzicht.
2b. Stel eisen te stellen aan een account en/of een apparaat voordat toegang tot Office365 services mogelijk is	Noodzakelijk	Deels gerealiseerd	Voor Devices van de IRVN is conditional access geregeld. Wordt regionaal georganiseerd. Opgenomen in nieuwe maatregelen-overzicht.
2c. Mail blijven routeren via KPN voor gebruik Suwinet mail en toepassing beveiligingsstandaarden.	Noodzakelijk	Gerealiseerd	Loopt niet meer via KPN (I-Zorg) We kunnen Suwinet niet benaderen via Exchange Online. Er is een CISKO appliance die zorgt voor alles wat Exchange Online ondersteunt. Suwinet heeft een connectie met Exchange Online maar het is geregeld. De standaarden worden nageleefd.
2d. Aanvullende technische maatregelen gebruik Zorgmail	Noodzakelijk	Gerealiseerd	Is geregeld via Zyvver.
3b. Zet de telemetrie op het niveau 'Neither'	Aanbevolen	Gerealiseerd	
3c. Zet het telemetrieniveau in Windows 10 Enterprise op Security (Beveiliging)	Aanbevolen	Gerealiseerd	
3d. Schakel het Customer Experience Improvement Programma (CEIP) uit	Aanbevolen	Gerealiseerd	
3f. Scheidt tenants in de regio of creëer een eigen tenant voor de gemeente Nijmegen	Aanbevolen	Gerealiseerd	
3g. Blokkeer het synchroniseren van activiteiten van gebruikers door middel van de "Timeline" functionaliteit	Niet noodzakelijk	Gerealiseerd	
4a. Zet LinkedIn-integratie uit voor Microsoft werknemer accounts	Aanbevolen	Gerealiseerd	
5a. Upgrade naar versie 1905 of hoger van Office 365 ProPlus	Aanbevolen	Gerealiseerd	
5b. Actualiseer het bestaande werknemers privacybeleid	Aanbevolen	Deels gerealiseerd	Privacyverklaring externe medewerkers verschoven tot na de tenantscheiding. Opgenomen in nieuwe maatregelen-overzicht.

Maatregelen	Advies FG	Status	Toelichting
3a. Verbiedt centraal het gebruik van de Controller Connected Experiences	Niet noodzakelijk	Niet gerealiseerd	Tooltjes binnen Office die aanbevelingen voor je doet. Moet in de toekomst uitgezocht en beleid voor ontwikkeld worden. IRVN zet het standaard uit. Het gaat pas open als een gemeente daarvoor een verzoek doet. Opgenomen in nieuwe maatregelen-overzicht.
3e. Gebruik Customer Lockbox en Customer Key, afhankelijk van de gevoeligheid van de inhoudelijke gegevens	Niet noodzakelijk	Niet gerealiseerd	Hiervoor is een E5 licentie nodig.
5c. Voer DPIA's uit voorafgaand aan het gebruik van Workplace Analytics and Activity Reports in het Microsoft 365 admin center en voordat werknemers gebruik kunnen maken van MyAnalytics and Delve	Niet noodzakelijk	Niet gerealiseerd	Er moeten afspraken gemaakt worden over wie dat soort verzoeken mag doen aan de IRVN. Die afspraken moeten op papier gezet worden en door de gemeente(s) en de IRVN vastgesteld en geïmplementeerd. In een andere vorm opgenomen in nieuwe maatregelen-overzicht.
5d. Stel beleid op om werknemers te waarschuwen dat zij de mobiele Office apps en de Controller Connected Experiences niet mogen gebruiken, totdat de hoge risico's zijn gemitigeerd	Niet noodzakelijk	Niet gerealiseerd	

3.3 Is er sprake van stelselmatige monitoring?

Nee, al is de mogelijkheid er wel. Via Viva kan MS365 gebruikt worden om medewerkers te monitoren. Deze functionaliteit wordt echter niet toegepast bij de gemeente Nijmegen.

3.4 Is er sprake van matching of samenvoeging van datasets?

Nee

3.5 Is er sprake van innovatief gebruik van data?

Nee; er zijn in ieder geval geen plannen om met innovatieve componenten van MS365, zoals CoPilot, te gaan werken. Als CoPilot gebruikt gaat worden is er aanvullende besluitvorming nodig en ook een (aanvullende) DPIA.

4. Gegevens

4.1 Gaat het om een eenmalige uitwisseling van persoonsgegevens of structureel?

De uitwisseling van gegevens is structureel, maar er is hiervoor geen frequentie of termijn aan te geven.

4.2 Welke persoonsgegevens worden verwerkt?

Er zullen verschillende vormen van vastlegging voor kunnen komen – denk hierbij aan e-mails, afspraken, acties, notities, documenten, videogesprekken, chats etc. In deze verschillende vormen van vastlegging kunnen in potentie verschillende vormen van persoonsgegevens worden vastgelegd. Een onvermijdelijke vorm van verwerking van persoonsgegevens zijn de contactpersonen gegevens. Het uitgangspunt is dat er zeker geen bijzondere persoonsgegevens verwerkt zullen worden. Hiervoor is MS365 niet bedoeld.

Diagnostische gegevens bevatten in ieder geval apparaatgegevens. Denk hierbij het unieke identificatienummer van een mobiele werkplek (laptop). Deze kunnen, met name bij mobiele apparaten, dus als zodanig te herleiden zijn tot een individueel persoon. Hoewel Microsoft weinig informatie geeft over deze verwerking staat wel inmiddels vast dat Microsoft geen inhoudelijke of functionele gegevens verzamelt. Daarmee is deze verwerking in principe een gewone gegevensverwerking.

4.3 Is de beoogde verwerking proportioneel?

Zoals beschreven is doel van het gebruik van MS365 het verbeteren van digitaal samenwerken. Zonder gegevensverwerking in MS365 is de gegevensverwerking rond voorbereiden van beleid, projectuitvoering en overleg minder veilig en minder rechtmatig. De werkwijze zonder gebruik van MS365 is het gebruik van documentopslag op gemeenschappelijke netwerkschijven, met een zeer beperkte bescherming en geen mogelijkheid tot vernietiging. Met de invoering van MS365 en het invoeringstraject er omheen zal privacybescherming en archivering in ieder geval beter worden.

Hoewel verwerking van persoonsgegevens niet uit te sluiten is, zullen bij de gekozen doelen van samenwerking (beleid, projecten, overleg, kennisdeling) relatief weinig persoonsgegevens verwerkt worden. Wanneer Team(sites) persoonsgegevens bevatten, dient deze besloten gemaakt te worden en alleen medewerkers toegang te hebben die vanuit hun functie noodzakelijk bij deze gegevens moeten kunnen (volgt uit het informatiebeheerplan). Pas wanneer er een persoonsgegeven inkomt kan er in het specifieke proces een afweging worden gemaakt. Dit kan niet globaal beoordeeld worden.

4.4 Is de beoogde verwerking subsidiair?

Ook in dit geval kan er met betrekking tot de verwerking van persoonsgegevens alleen een afweging gemaakt worden in het specifieke proces. Dit kan niet globaal beoordeeld worden. Wat betreft de keuze voor MS365: Op basis van een scenario-model is uitgezocht hoe het ICT-landschap van kantoorautomatisering (KA) zich de komende jaren zal ontwikkelen. Hieruit is naar voren gekomen dat het aanbod in de markt zeer beperkt zal blijven en dat gemeentes steeds meer eenzelfde platform willen gebruiken, waardoor 2 scenario's het meest waarschijnlijk zijn: de "happy lock-in", waarin we volledig in het platform gaan investeren en "one size fits all. Or none. For now.", waarbij we de lock-in effecten zo klein mogelijk proberen te houden. Beide scenario's sluiten in het huidige ICT-landschap uit dat we met een open source-variant verder gaan.

Bovendien is het zo dat primaire taakuitvoering zoveel mogelijk plaats dient te vinden in eigen procesapplicaties, en dus niet in MS365. Denk bijvoorbeeld aan de Suite voor het sociaal domein, of JeugdVolgSysteem (JVS). Op deze eigen processen en bijbehorende applicaties worden losse DPIA's gemaakt.

4.5 Worden de persoonsgegevens buiten de EER gebruikt?

In beperkte mate, met name om de performance van het MS365-platform te verbeteren. Met Microsoft is de EU Boundary Act vastgesteld, die verwerking zoveel mogelijk binnen de grenzen van de EU laat plaatsvinden. Afspraken hierover zijn op Europees en rijksniveau gemaakt.

5. Partijen

5.1 Welke partijen zijn bij de verwerking betrokken?

In structurele zin zijn de volgende partijen betrokken bij het functioneren van MS365:

- ICT bedrijf Rijk van Nijmegen - verwerker
- Microsoft - verwerker/verantwoordelijke
 - Microsoft is voor gemeente Nijmegen in principe verwerker. Zij verwerken echter ook diagnostische (persoons)gegevens om hun eigen dienstverlening te verbeteren. Voor dat deel zijn ze zelf verwerkingsverantwoordelijke.
- Gemeente Nijmegen – verwerkingsverantwoordelijke
- SplitVision – verwerker (archiveren)

5.2 Welke overeenkomsten worden aangegaan als gevolg van die rollen?

Zie hiervoor de bijlagen. De VNG heeft namens Nederlandse gemeente een Juridisch Framework met Microsoft afgesloten, dat dient als een verwerkersovereenkomst.

6. Zorgplicht

6.1 Op welke wijze is het project en haar analyses in begrijpelijke taal uit te leggen?

De gemeente Nijmegen gebruikt een digitaal samenwerkingsplatform waar documenten, notities en andere bestanden opgeslagen worden, e-mails en chats verstuurd worden en de mogelijkheid is om te video vergaderen. Hierbij wordt het verwerken van persoonsgegevens geminimaliseerd, maar is niet uit te sluiten.

6.2 Op welke wijze(n) worden betrokkenen geïnformeerd?

Er zijn drie categorieën betrokkene te onderscheiden waarop deze gegevensverwerking van toepassing is. Enerzijds betreft dit *medewerkers* (zowel in dienst van als ingehuurd door) en vrijwilligers van de gemeente Nijmegen. In ieder geval alle medewerkers met een inlogaccount op de KA omgeving. De medewerkers zijn op de hoogte van de overstap naar MS365. Ook van medewerkers van partnerorganisaties waar we mee samenwerken worden in beperkte zin persoonsgegevens verwerkt.

Anderzijds betreft dit *burgers* van wie wij (potentieel) persoonsgegevens verwerken in applicaties binnen het MS365-platform. Een laatste categorie zijn *raadsleden* en fractiemedewerkers. Er wordt alleen naar deze laatste groep buiten toe gecommuniceerd over de overstap.

6.3 Op welke manier zijn de rechten van betrokkenen geborgd in het proces?

Met de invoering van MS365 worden de mogelijkheden om rechten van betrokkenen, zoals inzage en gegevenswisseling te borgen groter. MS365 biedt via de tool eDiscovery de mogelijkheid om integraal een zoekopdracht uit te kunnen voeren over alle applicaties binnen met MS365-platform, waarmee voldaan kan worden aan een AVG-inzage verzoek.

Binnen het project moet nog overwogen worden hoe de gemeente Nijmegen deze mogelijkheden gaat inzetten. Afhankelijk van de licentievorm biedt deze tool beperkte tot uitgebreide mogelijkheden. Het huidige contract met Microsoft is gebaseerd op de E3-licentievorm. Dat betekent dat na overgang gezocht kan worden in alle mailboxen en Exchange-mappen en dat deze zoekresultaten in een “case” bewaard en geëxporteerd kunnen worden. De duurdere E5-licentie verbetert het zoeken, waardoor betere resultaten ontstaan en de privacyinbreuk van het zoeken zelf beperkter wordt. Hiervoor wordt echter wel gebruik gemaakt van AI-technieken. De E3-vorm van eDiscovery lijkt daarom afdoende, echter dient deze wel ingericht te worden voor gebruik door afzonderlijke gemeentes en ingepast in de huidige procedure voor rechten van betrokkenen. Op dit punt is een overgang naar een duurdere E5 licentie dan ook niet nodig.

7. Informatiebeveiliging en vernietiging

7.1 Hoe lang worden de gegevens bewaard?

Bewaren en vernietigen van persoonsgegevens wordt nu voor veel taken gemakkelijker. De regimes hiervoor worden gekoppeld aan de verschillende vormen van flexibel samenwerken die we onderscheiden:

Soort team	Pre fix	Ingang sluiten team	Zaaktype code	Resultaat type (keuze na sluiten team)	Bewaren of vernietigen	Grondslag selectielijst
Beleid maken	B	Na vervallen beleid of geldigheidsduur of afbreken beleid	B0777	Vastgesteld interne werking	Vernietigen na 10 jaar	2.1
				Vastgesteld externe werking	Bewaren	2.1.1
				Niet doorgegaan	Vernietigen na 5 jaar	2.2
				Tussentijds afgebroken	Vernietigen na 1 jaar	2.4
Project uitvoeren	P	Na afronden project	B0700	Vastgesteld externe werking	Bewaren	2.1.1

Soort team	Pre fix	Ingang sluiten team	Zaaktype code	Resultaat type (keuze na sluiten team)	Bewaren of vernietigen	Grondslag selectielijst
				Niet doorgegaan	Vernietigen na 5 jaar	2.2
				Tussentijds afgebroken	Vernietigen na 1 jaar	2.4
				Uitgevoerd (vaar)weg	Bewaren	14.1.2
				Uitgevoerd gedenkteken	Bewaren	14.1.3
				Uitgevoerd bouw- en woonrijp	Bewaren	14.1.4
				Uitgevoerd gebouw	Bewaren	14.1.5
				Uitgevoerd kunstobject openbare ruimte	Bewaren	14.1.6
				Uitgevoerd overig	Vernietigen na 10 jaar	14.1
Structureel overleggen	O	Na einde jaar	B1366	Intern overleg (verwerkt)	Vernietigen na 5 jaar	19.1.11
Kennisbank	K	Na uitvoering of verstrijken relevantie	B1320	Uitgevoerd	Vernietigen na 1 jaar	20.1

Vernietiging van teams en sites verloopt volgens de bovenstaande vernietigingstermijnen die per sitesjabloon zijn vastgelegd en daarmee per team of site (documentsets) worden uitgevoerd.

1. Als een team wordt afgesloten, dan dient een resultaattype aangegeven te worden, op basis waarvan definitief bepaald kan worden of bewaard of vernietigd moet worden en hoe lang.
2. Na afsluiten wordt het Team verwijderd en de documentset overgezet naar een archiefmodule binnen Sharepoint, waardoor de documenten nog steeds te vinden zolang de vernietigingstermijn nog niet af is gelopen.
3. Continu worden vernietigingslijsten gemaakt van documentsets waarvan de vernietigingstermijn is afgelopen. Deze worden beoordeeld en vastgesteld, waarna vernietiging kan plaatsvinden en een verklaring van vernietiging wordt opgesteld.
4. Een beperkt deel van de teams of sites zullen eeuwig bewaard dienen te blijven (afhankelijk van het zaaktype en het resultaat van de samenwerking). Dat betekent dat deze Teams of Sites in het geheel overgedragen dienen te worden naar het e-Depot, door middel van een handmatige export of een koppeling.

Het volledige vernietigingsprotocol is te vinden in het informatiebeheerplan voor MS365¹.

E-mails horen zoveel mogelijk bij de zaak in het zaakdossier opgeslagen en met het dossier bewaard of vernietigd te worden. Dat kan in Teams, SharePoint-site of een applicatie buiten MS365 zijn (Corsa of een taakspecifieke applicatie). Voor Corsa hebben we al een plugin beschikbaar, voor taakspecifieke applicaties waarin dossieropbouw plaatsvindt (bestandsomgevingen) dient dat overwogen te worden. Medewerkers dienen ervoor te zorgen dat er geen belangrijke e-mails en documenten alléén in hun e-mailpostbus te vinden zijn. E-mails met privacygevoelige informatie dienen zo snel mogelijk in het juiste zaakdossier geplaatst te worden en/of uit de e-mailpostbus verwijderd te worden.

E-mails die in Outlook blijven staan worden op een meer simpele wijze bewaard of vernietigd:

- Alle medewerkers mogen onbelangrijke en persoonlijke e-mails nog steeds zelf vernietigen, als ze uit dienst of met pensioen gaan en ook tussentijds.

¹ [Informatiebeheerplan MS365.docx](#)

- Alle overgebleven e-mails worden na 7 jaar vernietigd, ook als medewerkers vertrokken zijn bij de gemeente Nijmegen, of met pensioen gegaan zijn. Het beheer van deze “wees”-mailboxes van vertrokken medewerkers (voor bijv. toegang bij informatie in het kader van informatieverzoeken) dient bij hiertoe gemachtigde secretariaten en BDI te komen liggen.

E-mails van medewerkers die een sleutelfunctie bekleden worden eeuwig bewaard, voor de tijd dat deze medewerkers de sleutelfunctie hebben bekleed. Ook dit is vastgesteld via de selectielijst e-mailbewaring, waarin een aantal functionarissen zijn beschreven. Het overzicht aan sleutelfuncties staat beschreven in het informatiebeheerplan voor MS365².

Met de overstap naar MS365 worden langzaam aan ook de netwerkschijven uitgefaseerd. De documenten daarin worden opgedeeld in 3 opties:

- Te vernietigen
- Te archiveren
- Te verplaatsen naar MS365. De documenten die verplaatst worden vallen daarna onder de hierboven beschreven regimes.

7.2 Wie is verantwoordelijk voor de vernietiging van de gegevens?

Eigenaren van Teams, Sharepointsites en e-mailpostbussen zijn verantwoordelijk voor het op tijd afsluiten ervan. Op dat moment kan vernietiging van gegevens pas uitgevoerd worden. In het informatiebeheerplan voor MS365 is een vernietigingsprotocol beschreven. Op dit moment is echter nog niet bepaald welk organisatieonderdeel verantwoordelijk wordt voor het daadwerkelijk vernietigen van gegevens.

7.3 Is er een vastgesteld normenkader van toepassing op deze gegevensverwerking?

Bij de inrichting van MS365 wordt gebruik gemaakt van kaders op het gebied van informatiebeveiliging, privacybescherming en archivering.

7.4 Hoe worden de gegevens beveiligd? Hoe is het toezicht daarop georganiseerd?

De organisatie van beveiliging ligt voor het grootste (technische) deel bij het ICT-bedrijf Rijk van Nijmegen. Voor het organisatorische en technische deel ligt het toezicht bij de CISO en de security officers van Bureau Ontwikkeling I&A. Landelijke DPIA's: [Nieuwe DPIA voor de Rijksoverheid en universiteiten op Microsoft Teams, OneDrive en SharePoint Online](#) | [Privacy Company Blog](#)

Er worden in MS365 2 niveaus van toegankelijkheid en vertrouwelijkheid mogelijk gemaakt:

- Openbaar (als je toegang hebt tot de Nijmeegse omgeving, dus eigenlijk intern openbaar)
- Besloten

We regelen toegankelijkheid en vertrouwelijkheid vooral op het niveau van Team(sites), met name voor besloten Team(sites). Intern openbare Team(sites) bevatten intern openbare documenten en bestanden, besloten Team(sites) bevatten (in principe) vertrouwelijke documenten en bestanden. Wanneer we een document vanuit een besloten Team(site) willen delen met iemand, dan dient deze lid gemaakt te worden van dit/deze Team(site). Een document of bestand in een *intern openbaar* Team(site) kan wel gedeeld worden buiten MS365 zonder dat deze persoon lid is van een Team(site).

² [Informatiebeheerplan MS365.docx](#)

Rol	Toelichting rol	Mogelijkheden binnen/rond (intern) openbaar team	Mogelijkheden binnen besloten team
Gast	<i>Derde, geen medewerker van gemeente Nijmegen</i>	Op uitnodiging: <ul style="list-style-type: none"> Lid worden van een team(site) Toegang krijgen tot specifieke documenten / bestanden 	Op uitnodiging: <ul style="list-style-type: none"> Lid worden van een team(site)
Medewerker (zonder lid te zijn van een team)	Iedereen met een MS365-account, ook inhuur	Via "Lid worden" of overzichtspagina Sharepoint: <ul style="list-style-type: none"> Overzicht over alle intern openbare teams Mogelijkheid om lid te worden (zonder goedkeuringsproces) Via zoeken: <ul style="list-style-type: none"> Vinden van alle documenten / bestanden Open en bewerken van alle documenten / bestanden Via Sharepoint: <ul style="list-style-type: none"> Documenten/bestanden bewerken, verwijderen en delen buiten het team of de site (ook naar derden) 	Op uitnodiging: <ul style="list-style-type: none"> Lid worden van een team(site)
Teamlid	<i>Door verantwoordelijke of beheerder team lid gemaakte medewerker of gast</i>	Via Teams en Sharepoint: <ul style="list-style-type: none"> Overzicht over teams waar medewerker lid van is Open en bewerken van alle documenten / bestanden Documenten/bestanden bewerken, verwijderen en delen buiten het team of de site (ook naar derden) 	Via Teams en Sharepoint: <ul style="list-style-type: none"> Overzicht over teams waar medewerker lid van is Open en bewerken van alle documenten / bestanden Documenten/bestanden bewerken, verwijderen en delen naar andere leden team(site)
Eindverantwoordelijke / beheerder	<i>Beide rollen zijn technisch gezien "eigenaar"</i>	<ul style="list-style-type: none"> Gasten toevoegen aan een team(site) De machtigingen van de teams instellen voor kanalen, tabs en connectors (apps en koppelingen) 	<ul style="list-style-type: none"> Gasten en leden toevoegen aan een team(site) De machtigingen van de teams instellen voor kanalen, tabs en connectors (apps en koppelingen)

Risico's

8.1 Benoem hieronder de risico's voor betrokkenen door de gegevensverwerking

Het doel van een DPIA is om op grond van de geïnventariseerde risico's te komen tot maatregelen ter voorkoming dat de risico's zich voor de Nijmeegse situatie voordoen. De DPIA biedt daarnaast de mogelijkheid om de maatregelen te plannen, en om vervolgens verantwoording over de maatregelen en de effecten daarvan te kunnen afleggen. In dit hoofdstuk wordt gekeken wat de risico's zijn op het werkelijk worden van de dreigingen zoals deze in de matrix worden beschreven. Op basis daarvan worden in paragraaf 2 maatregelen beschreven die aanbevolen worden om de risico's te voorkomen of de effecten van die risico's voor de gemeente Nijmegen te mitigeren. Risico is geformuleerd in termen van de waarschijnlijkheid dat zich het risico voordoet (kans), afgezet tegen de hoeveelheid schade of gevolgen die het risico kan hebben (de impact). Hiervoor wordt gebruik gemaakt van de volgende categorieën:

Waarschijnlijkheid	Impact op de organisatie
Onaannemelijk, qua frequentie bijv. eens per jaar	Niet van belang, in kosten (schade of verlies): 0,- tot 10.000,-
Sporadisch, qua frequentie bijv. eens per halfjaar	Klein, in kosten (schade of verlies): 10.000,- tot 100.000,-
Eventueel, qua frequentie bijv. eens per kwartaal	Groot, in kosten (schade of verlies): 100.000,- tot 1.000.000,-
Waarschijnlijk, qua frequentie bijv. maandelijks	Enorm, in kosten (schade of verlies): 1000.000,- tot 10.000.000,-
Vrijwel zeker, qua frequentie bijv. wekelijks of vaker	Desastreus, in kosten (schade of verlies): 10.000.000,- en hoger

Het risico wordt berekend door de waarschijnlijkheid in scores van 1-5 te vermenigvuldigen met het niveau van de impact van de dreiging, die ook van 1-5 lopen (risico = kans x impact). Vanaf een score van 3 hebben we te maken met een midden risico niveau. Vanaf een score van 12 hebben we te maken met een hoog risico niveau.

	Risico impact				
Risico kans	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

In opdracht van SLM Rijk, de centrale onderhandelaar voor producten en diensten van Microsoft, Google en Amazon Web Services voor de rijksoverheid, en voor SURF, de centrale IT-inkooporganisatie voor Nederlandse hogescholen en universiteiten, zijn herhaaldelijk DPIA's uitgevoerd³. De uitkomst van de laatste DPIA, na herhaald overleg met Microsoft, is dat er geen bekende hoge risico's meer zijn voor de verwerking van diagnostische gegevens.

Hieronder volgt een matrix met de mogelijke risico's die zich voor kunnen doen bij het gebruik van MS365. Dit wordt gevolgd door een score op waarschijnlijkheid en impact waarvan de betekenis hierboven is beschreven. De vermenigvuldiging hiervan leidt tot de gehele risicoscore aan de hand waarvan een risiconiveau kan worden afgeleid.

Te beschermen risico (dreiging)	Score waarschijnlijkheid	Score impact	Risicoscore	Risico niveau
Persoonsgegevens kunnen voor medewerkers buiten het specifieke Team en gasten toegankelijk zijn, indien in niet-besloten omgevingen opgeslagen	5	4	20	Hoog

³ <https://www.privacycompany.eu/nl/blog/nieuwe-dpia-voor-de-rijksoverheid-en-universiteiten-op-microsoft-teams-onedrive-en-sharepoint-online>

Lijsten met persoonsgegevens kunnen voor te veel medewerkers en Microsoft toegankelijk worden, indien niet verplaatst naar een procesapplicatie. Bijvoorbeeld door data persoonsgegevens in een Team staan dat voor iedereen inzichtelijk is.	4	4	16	Hoog
Rechten van betrokkenen kunnen niet (goed) voldaan worden (bijvoorbeeld de gemeente kan bij een inzageverzoek niet goed alle persoonsgegevens naar boven halen)	3	5	15	Hoog
Persoonsgegevens uit MS365 kunnen worden opgeslagen op onbeheerde apparaten (zoals een privé computer van een medewerker) en daarmee een datalek veroorzaken	5	2	10	Midden
Inhoudelijke (persoons)gegevens verwerkt in de EU zijn toegankelijk voor Microsoft, indien niet versleuteld, aangezien ze worden opgeslagen in de cloud van Microsoft.	4	2	8	Midden
Doorgifte diagnostische en beveiligingsgegevens buiten de EU	4	1	4	Laag
Diagnostische gegevens kunnen gebruikersnaam en/of het e-mailadres van medewerkers bevatten	4	1	4	Laag
Gebrek aan transparantie over gebruik diagnostische gegevens door Microsoft en beperkte inzage in Required Service Data	4	1	4	Laag
Gebrek aan controle op verstrekking van persoonsgegevens aan Microsoft en derde partijen die verwerkingsverantwoordelijken zijn	4	1	4	Laag
Personeelsvolgsysteem kan eenchilling effect als gevolg hebben. Dit is een effect op de houding van medewerkers wanneer hun gedrag gemonitord wordt. Ze kunnen dit als niet prettig ervaren. Een dergelijke monitoring kan bijvoorbeeld een resultaat hebben op hun prestatiebeoordeling. Microsoft biedt de mogelijkheid om namen van medewerkers te pseudonimiseren, maar het is niet duidelijk of dit effect heeft op de ruwe datalogs van Microsoft.	4	1	4	Laag

Om te bepalen welke maatregelen noodzakelijk zijn om de privacyrisico's te mitigeren, wordt niet alleen gekeken naar de ernst van het privacyrisico (hoog midden of laag), maar ook wat voor effect de voorgenen maatregel op de vermindering van het risico heeft, én wat de impact het invoeren van de maatregel heeft op de organisatie (proportionaliteit). Dus bij een beperkt effect van de voorgestelde maatregel op het privacyrisico, maar met een (te) grote impact op de organisatie kan op een maatregel als niet noodzakelijk worden geadviseerd, ook al in het privacyrisico zelf hoog.

Risico niveau	Effect maatregel op risico	Impact op organisatie	Advies
Midden	Beperkt	Geen	Noodzakelijk

Laag	Groot	Geen	Noodzakelijk
Hoog	Beperkt	Geen	Noodzakelijk
Hoog	Groot	Geen	Noodzakelijk
Hoog	Groot	Beperkt	Noodzakelijk
Midden	Groot	Geen	Noodzakelijk
Midden	Groot	Beperkt	Noodzakelijk
Hoog	Beperkt	Beperkt	Aanbeveling
Hoog	Groot	Groot	Aanbeveling
Midden	Beperkt	Beperkt	Aanbeveling
Midden	Groot	Groot	Aanbeveling
Laag	Groot	Beperkt	Aanbeveling
Laag	Beperkt	Geen	Aanbeveling
Hoog	Beperkt	Groot	Accepteer risico – niet uitvoeren
Midden	Beperkt	Groot	Accepteer risico – niet uitvoeren
Laag	Beperkt	Beperkt	Accepteer risico – niet uitvoeren
Laag	Beperkt	Groot	Accepteer risico – niet uitvoeren
Laag	Groot	Groot	Accepteer risico – niet uitvoeren

8.2 Benoem de maatregelen die nog noodzakelijk (en aanbevolen) zijn

Mogelijke maatregel	Type maatregel	Te beschermen risico (dreiging)	Risico niveau	Effect op risico	Impact	Advies	Fase 1 (J/N)	Toelichting
Geef instructie aan medewerkers en leidinggevenden over een veilig en privacybeschermend gebruik van Teams, Sharepoint, Onedrive en Outlook	Organisatorisch	Persoonsgegevens kunnen voor niet-noodzakelijke medewerkers en gasten toegankelijk zijn, indien in niet-besloten omgevingen opgeslagen	Hoog	Groot	Beperkt	Noodzakelijk	J	
Laat medewerkers en gastgebruikers privacyregels accepteren door middel van voorwaarden die door Azure AD worden opgelegd	Technisch	Inhoudelijke (persoons)gegevens verwerkt in de EU zijn toegankelijk voor Microsoft, indien niet versleuteld	Midden	Beperkt	Beperkt	Aanbeveling	J	Wordt nu gebouwd
Stel bij het gebruik van OneDrive en SharePoint beleidsregels op om te voorkomen dat bestandsnamen en bestandspaden persoonlijke gegevens bevatten	Organisatorisch	Doorgifte diagnostische en beveiligingsgegevens buiten de EU	Laag	Beperkt	Geen	Aanbeveling	J	Aanpassing informatiebeheerplan en instructie. Op dit moment 1 voorbeeld.
Beperk de toegang tot apps van derde partijen in de Teams appstore, sta apps alleen toe na een intakeproces	Technisch	Gebrek aan controle op verstrekking van persoonsgegevens aan Microsoft en derde partijen die verwerkingsverantwoordelijken zijn	Laag	Groot	Beperkt	Aanbeveling	J	
Schakel de functionaliteit Teams Analytics & rapporten uit, gebruik Viva Insights niet	Technisch	Personeelsvolgsysteem: chilling effect	Laag	Groot	Geen	Noodzakelijk	J	

Mogelijke maatregel	Type maatregel	Te beschermen risico (dreiging)	Risico niveau	Effect op risico	Impact	Advies	Fase 1 (J/N)	Toelichting
Gebruik multifactor authenticatie voor externen	Technisch	Persoonsgegevens kunnen voor niet-noodzakelijke medewerkers en gasten toegankelijk zijn, indien in niet-besloten omgevingen opgeslagen	Hoog	Beperkt	Beperkt	Aanbeveling	N	
Monitor op een veilig en privacybeschermend gebruik van Teams, Sharepoint, Onedrive en Outlook	Technisch	Persoonsgegevens kunnen voor niet-noodzakelijke medewerkers en gasten toegankelijk zijn, indien in niet-besloten omgevingen opgeslagen	Hoog	Groot	Beperkt	Noodzakelijk	N	Monitoring is op verschillende wijze mogelijk. Noodzaak daarvoor en de aspecten waarop gemonitord moet worden is beschreven in het informatiebeheerplan.
Gebruik eDiscovery binnen E3 voor aanvragen mbt rechten van betrokkenen	Technisch	Rechten van betrokkenen kunnen niet voldaan worden	Midden	Groot	Beperkt	Noodzakelijk	N	In beperkte vorm mogelijk binnen de E3-licentie via de eDiscoverytool. Deze moet wel ingericht worden en ingepast in het werkproces.
Formaliseren beheerorganisatie voor tijdige vernietiging en controle op autorisatie en beveiliging	Organisatorisch	Persoonsgegevens kunnen voor niet-noodzakelijke medewerkers en gasten toegankelijk zijn, indien in niet-besloten omgevingen opgeslagen	Hoog	Groot	Groot	Aanbeveling	N	
Beheren en beveiligen van alle (gemeentelijke) apparaten waar MS365-gegevens op opgeslagen kunnen worden en zorgen dat alleen daar (persoonsgevoelige) gegevens opgeslagen kunnen worden.	Technisch	Persoonsgegevens uit MS365 kunnen worden opgeslagen op onbeheerde apparaten en daarmee een datalek veroorzaken	Midden	Groot	Groot	Aanbeveling	N	Alle apparaten (incl. iPhones) van de gemeente moeten onder beheer komen, om dit door te kunnen voeren. Op andere apparaten kan alleen de webversie van MS365 gebruikt worden.

Mogelijke maatregel	Type maatregel	Te beschermen risico (dreiging)	Risico niveau	Effect op risico	Impact	Advies	Fase 1 (J/N)	Toelichting
Schakel E2EE standaard in voor 1-op-1 gesprekken in Teams, en instrueer eindgebruikers om ook E2EE in te schakelen	Technisch	Inhoudelijke (persoons)gegevens verwerkt in de EU zijn toegankelijk voor Microsoft, indien niet versleuteld	Midden	Groot	Groot	Aanbeveling	N	Teams E2EE is een Teams Premium feature, vereist aanvullende licenties. Hiervoor is een intake nodig.
Gebruik pseudoniemen in de Azure AD voor medewerkers waarvan de werkidentiteit vertrouwelijk moet blijven	Organisatorisch	Doorgifte diagnostische en beveiligingsgegevens buiten de EU	Laag	Groot	Beperkt	Aanbeveling	N	
Gebruik geen SMS voor authenticatie om de doorgifte te voorkomen van niet-versleutelde mobiele telefoonnummers naar derde landen. Gebruik in plaats daarvan de Authenticator app of een hardware token	Technisch	Doorgifte diagnostische en beveiligingsgegevens buiten de EU	Laag	Groot	Beperkt	Aanbeveling	N	
Gebruik Double Key Encryption voor bestanden met gevoelige of bijzondere persoonsgegevens die zijn opgeslagen in SharePoint/OneDrive. Hieronder vallen ook opnamen van Teams-gesprekken. Gebruik Customer Lockbox om andere opgeslagen persoonsgegevens te beschermen.	Technisch	Inhoudelijke (persoons)gegevens verwerkt in de EU zijn toegankelijk voor Microsoft, indien niet versleuteld	Midden	Beperkt	Groot	Accepteer risico – niet uitvoeren	N	Double Key Encryption en Customer Lockbox vereisen een duurdere E5 licentie
Gebruik pseudoniemen in de Azure AD voor alle medewerkers	Organisatorisch	Doorgifte diagnostische en beveiligingsgegevens buiten de EU	Laag	Groot	Groot	Accepteer risico – niet uitvoeren	N	

Mogelijke maatregel	Type maatregel	Te beschermen risico (dreiging)	Risico niveau	Effect op risico	Impact	Advies	Fase 1 (J/N)	Toelichting
Gebruik Microsofts inzagetool voor beheerders om toegang te krijgen tot diagnostische gegevens, en vergelijk die met een incidentele analyse van het netwerkverkeer	Technisch	Gebrek aan transparantie over telemetriegegevens en beperkte inzage in Required Service Data	Laag	Beperkt	Beperkt	Accepteer risico – niet uitvoeren	N	
Schakel de Aanvullende Optionele Verbonden Ervaringen uit (connected experiences)	Technisch	Gebrek aan controle op verstrekking van persoonsgegevens aan Microsoft en derde partijen die verwerkingsverantwoordelijken zijn	Laag	Groot	Groot	Accepteer risico – niet uitvoeren	N	Connected Experiences in Office (=staat nu AAN) kan via een change worden uitgeschakeld. Een aantal privacybeschermende tools kan na inschakelen niet meer gebruikt worden, zoals information rights management of gevoeligheidlabels. Een aantal activiteiten levert foutmeldingen op, zoals het openen van een Word-document.

8.3 Wat is het restrisico dat overblijft?

Een deel van de geconstateerde risico's is te weerbarstig om volledig wel te krijgen met maatregelen (het effect van maatregelen op het risico is beperkt), ofwel te laag om met impactvolle maatregelen te beheersen. In het eerste geval zal het risico deels blijven bestaan, in het tweede geval geheel.

Uit het informatiebeheerplan volgt dat wanneer Team((sites) persoonsgegevens bevatten, dienen deze besloten gemaakt te worden en alleen medewerkers toegang te hebben die vanuit hun functie noodzakelijk bij deze gegevens moeten kunnen. We hebben echter te maken met menselijk handelen en het kan voorkomen dat er persoonsgegevens in een niet besloten Teams omgeving terecht komen.

Omgang met aanbevolen maatregelen beschrijven

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1