

DPIA Exchange Online

Rob Haans
Stijn Verhagen
Niels de Jager

Versiebeheer:

Datum	Versie	auditor
14-7-2020	0.01	5.1.2e
18-8-2020	0.03	5.1.2e
26-8-2020	0.03.1	5.1.2e
01-9-2020	0.0.3.2	5.1.2e
03-9-2020	0.0.3.3	5.1.2e
04-09-2020	0.0.3.4	5.1.2e
09-09-2020	0.0.3.5	5.1.2e
10-09-2020	0.0.4	5.1.2e
17-09-2020	0.0.4.1	5.1.2e
18-09-2020	0.0.5	5.1.2e
18-09-2020	0.0.5.1	5.1.2e
18-09-2020	0.0.5.2	5.1.2e
18-09-2020	0.9	5.1.2e
23-09-2020	0.9.1	5.1.2e
07-10-2020	0.9.2	5.1.2e
08-10-2020	0.9.3	5.1.2e
09-10-2020	1.0	5.1.2e
13-10-2020	1.1	5.1.2e
13-10-2020	1.1.1	5.1.2e

Inhoud

Totstandkoming DPIA, inleiding en scopebepaling	3
Scopebepaling	3
Out of scope	3
Stakeholders	4
Hoofdstuk 1 Exchange online en doelbinding	5
1.1 Persoonsgegevens en verantwoordelijkheid	5
1.2 Categorieën van gegevens	5
1.3 Gegevensverwerkingen buiten de EU	6
1.4 Tenant	6
Hoofdstuk 2 Borging rechten van betrokkenen	7
2.1 Betrokkenen (in de zin van de AVG)	7
2.2 Rechten van betrokkenen	7
Hoofdstuk 3 Privacydreigingen	8
3.1 Rechten van betrokkenen niet kunnen borgen	8
3.2 Onvoldoende privacy by design	8
3.3 Niet genoeg controle op subverwerkers en verwerkingen	8
3.4 Onvoldoende afspraken over verantwoordelijkheden en maatregelen	9
3.5 Overstap naar Exchange Online en DNSSEC, DANE	9
Hoofdstuk 4 Risicomitigatie en vertaling naar Nijmeegse situatie	10
Hoofdstuk 5: te nemen maatregelen	13
5.1 Noodzakelijke maatregelen	13
5.2 Aan te bevelen maatregelen	14
5.3 Niet-noodzakelijke maatregelen	14
Hoofdstuk 6 Advies Functionaris voor Gegevensbescherming	15

Totstandkoming DPIA, inleiding en scopebepaling

Binnen de regio Rijk van Nijmegen wordt er onderzoek gedaan naar mogelijke vervolgstappen om de ontwikkeling van de kantoorautomatisering (verder: KA) voort te zetten. Eén van de mogelijke stappen is de overstap naar Microsoft Exchange online (hierna: nieuwe KA-omgeving) en bij vervolg naar (eventueel) Office365 en Teams. Met deze eerste overstap wordt vrijwel de gehele werkomgeving verplaatst van het eigen datacenter (on premises) naar de cloud (met uitzondering van processpecifieke applicaties). Deze overstap brengt een groot aantal voordelen met zich mee, maar ook nieuwe privacyrisico's.

Dit onderzoek vormt de aanleiding om de privacyrisico's in beeld te brengen in de vorm van een DPIA¹ en op basis daarvan een gewogen afweging te kunnen maken binnen het onderzoek. Voorafgaand aan deze DPIA heeft het Rijk reeds een uitgebreide [DPIA](#)² uitgevoerd naar het gebruik van Office 365 binnen de kantooromgeving van de Rijksoverheid. De uitkomsten en voorgenomen maatregelen uit voornoemde DPIA vormen het uitgangspunt voor onderliggende DPIA gericht op de mogelijke KA van de gemeente Nijmegen. De basisvereisten vanuit de AVG worden hier daarom niet nogmaals herhaald. De belangrijkste conclusies uit de DPIA van het Rijk betreffen; dat na afronding van de DPIA het Rijk en Microsoft maatregelen overeengekomen zijn om de geconstateerde hoge risico's te beperken. Nadat Microsoft deze maatregelen heeft doorgevoerd, en mits overheidsorganisaties de aanbevelingen voor overheidsorganisaties in het DPIA rapport volgen, zijn in de DPIA geïdentificeerde hoge risico's zijn gemitigeerd. De aanbevelingen van de DPIA van het Rijk hebben wij in onderhavige DPIA dan ook als uitgangspunt genomen.

De antwoorden (en daarmee de huidige instellingen zoals geldend voor andere gemeenten die zijn aangesloten bij de IRVN) gelden alleen voor de Office365-omgeving, de Windows 10-systemen in één van beide domeinen (Azure AD/Karelstad-domein) en de Microsoft365 Apps.

Scopebepaling

Gelet op de huidige beleidsuitgangspunten betreffende de nieuwe KA houden we voor de DPIA een gefaseerde aanpak aan. De eerste fase betreft een onderzoek naar de overgang naar Exchange online. Dit met als vertrekpunt de DPIA zoals uitgevoerd door het Rijk. De fases daarop volgend zijn afhankelijk van de beleidsstandpunten en inzichten op dat moment en worden in samenspraak met de opdrachtgevers nader uitgewerkt en afgestemd. In de DPIA's zal er onderzoek worden gedaan naar de privacyrisico's die de nieuwe KA-omgeving met zich meebrengt. Daarnaast worden de risico's met betrekking tot informatiebeveiliging onderzocht. Als de risico's in kaart gebracht zijn wordt gezamenlijk met de IRVN gekeken naar mogelijke oplossingen c.q. privacy bevorderende maatregelen.

Out of scope

In de DPIA wordt enkel onderzoek gedaan naar de privacyrisico's van de overgang van Exchange on premises naar Exchange online. Hierbij wordt tevens onderzocht of de overgang privacyrisico's veroorzaakt bij het gebruik van specifieke applicaties. Een voorbeeld hiervan is het gebruik van Suwinet-mail. Deze applicatie vereist een aantal randvoorwaarden voor gebruik die in het geding komen bij de overgang naar de cloudomgeving. In deze DPIA wordt nadrukkelijk geen onderzoek gedaan naar beheersmatige of compatibiliteitsaspecten op applicatieniveau binnen Exchange online.

¹ Data Protection Impact Analyse

² <https://www.rijksoverheid.nl/documenten/rapporten/2020/06/30/data-protection-impact-assessment-office-365-for-the-web-and-mobile-office-apps>

Stakeholders

Er zijn diverse stakeholders bij de opdracht. Hieronder volgt een overzicht.

- Opdrachtgever DPIA – 5.1.2e (afdelingshoofd PIF – Gemeente Nijmegen)
- Opdrachtgever IRVN – 5.1.2e (CIO – Gemeente Nijmegen)
- Opdrachtnemer IRVN- 5.1.2e
- Leveranciersmanagement VNG – Microsoft: 5.1.2e (VNG/Servicecentrum gemeenten)
- Onderzoek leveranciersvoorwaarden Microsoft vs standaard verwerkersovereenkomst: 5.1.2e
- Veiligheidsonderzoek Nijmegen: 5.1.2e (coördinerend), 5.1.2e / 5.1.2e (adviserend)
- Veiligheidsaspecten beheer regio: 5.1.2e / 5.1.2e / 5.1.2e (IRVN)

Hoofdstuk 1 Exchange online en doelbinding

De huidige opzet van de e-mailomgeving waarin gewerkt wordt binnen de gemeente Nijmegen heeft een aantal beperkingen. Het belangrijkste voorbeeld hiervan is het gebrek aan continuïteit en toegankelijkheid tijdens serviceweekenden. Daarnaast zijn verschillende omliggende gemeenten binnen de gemeenschappelijke regeling ICT Rijk van Nijmegen overgestapt op Exchange Online en Office365, wat ervoor zorgt dat de iRvN twee e-mailsystemen draaiende moet houden, hetgeen leidt tot een onwenselijke situatie. De mogelijke overstap van gemeente Nijmegen naar Exchange Online en later eventueel Office365 moet ervoor zorgen dat de werkwijzes binnen het Rijk van Nijmegen onderling beter op elkaar zijn afgesteld en dat problematiek in de serviceweekenden verholpen wordt.

Microsoft Exchange en Outlook vormen samen de toepassing die nodig is om te kunnen e-mailen en vergaderingen te kunnen inplannen binnen de productrange van Microsoft. Outlook is de gebruikerstoepassing, Exchange is de beheerderstoepassing. Dit is onveranderd in de overgang naar Exchange Online en Office365.

Het belangrijkste doel van deze toepassing is het in onderlinge samenhang beheren van de volgende gegevens:

- e-mailberichten. Deze kunnen worden gecreëerd, verzonden, ontvangen en gearchiveerd;
- contactpersonen (naam, adres, e-mail, telefoonnummer etc.);
- afspraken in een elektronische agenda;
- taken of acties (to do list);
- losse aantekeningen (notes).

Om deze gegevens in een organisatie te kunnen delen en met elkaar samen te werken is Microsoft Exchange Server nodig. Zo kan bijvoorbeeld een centrale adressenlijst en distributielijst voor de verspreiding van e-mail worden bijgehouden, alsook voor het plannen van gezamenlijke meetings.

1.1 Persoonsgegevens en verantwoordelijkheid

Alle bovenstaande gegevens zijn ofwel rechtstreeks persoonsgegevens (contactpersonen) of kunnen –naar inhoud- (bijzondere) persoonsgegevens bevatten (de rest). De overgang naar Exchange online houdt vanuit AVG-perspectief in dat de bovenstaande gegevens verwerkt gaan worden door Microsoft op afstand, waar deze eerst in het eigen datacenter verbleven (on premises). Het college van Burgemeester en Wethouders van de gemeente Nijmegen is volgens de AVG verantwoordelijke voor de correcte en veilige gegevensverwerking van deze persoonsgegevens.

Daarnaast verzamelt Microsoft diagnostische gegevens om fouten op te lossen, apparaten up-to-date en veilig te houden en om eigen producten en diensten te verbeteren. Het gaat hierbij volgens Microsoft om 'Required service data' over het gebruik van de Connected Experiences, en gegevens over Essential Services, zoals authenticatie, telemetrie en controle van de licentie. Dit wordt bij alle Microsoft-toepassingen gedaan, via systeem-gegenereerde logboeken van gebeurtenissen op haar eigen servers en via de zogenaamde telemetrie-cliënt. Net als in Windows 10 heeft Microsoft software ingebouwd in de geïnstalleerde versies van Office die systematisch diagnostische (telemetrie-)berichten verzamelt op het apparaat van de gebruiker en regelmatig in batches verstuurt naar Microsoft's servers in de Verenigde Staten. Microsoft is voor deze verwerking de verantwoordelijke partij en heeft dat inmiddels ook onderkend.

1.2 Categorieën van gegevens

De primair verwerkte gegevens (e-mails, afspraken, acties, notities) kunnen in potentie alle vormen van (bijzondere) persoonsgegevens bevatten. Alleen van contactpersonen is vast te stellen dat het niet om bijzondere persoonsgegevens gaat.

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.

Een uitgebreid overzicht van categorieën van persoonsgegevens is te vinden in de bijlage³ van de DPIA die door het Rijk is uitgevoerd.

1.3 Gegevensverwerkingen buiten de EU

Het grootste deel van de gegevensverwerkingen rond Exchange online, met die van primair verwerkte gegevens vindt inmiddels plaats binnen Europa. De diagnostische (telemetrie-)gegevens worden in de VS opgeslagen, met name omdat daar deze gegevens geanalyseerd worden⁴. Ook voor het gebruik van de multifactor-authenticatie geeft Microsoft aan dat gebruik wordt gemaakt van servers buiten de EER in Amerika. Zie voor meer informatie de websites van Microsoft⁵. De huidige routing van de multifactor-authenticatie via servers in Amerika is meer problematisch geworden door de uitspraak van het Hof van Justitie. Hierin is het EU-VS privacy shield (privacyschild) ongeldig verklaard in de zaak Schrems II. Dat betekent dat organisaties in de EU geen persoonsgegevens aan de Verenigde Staten (VS) meer kunnen doorgeven op grond van het privacy shield. Volgens het Hof kunnen modelcontracten nog wel een geldige grondslag bieden voor doorgifte van gegevens naar landen buiten de EU. Maar alleen als een gelijkwaardig beschermingsniveau in de praktijk kan worden gewaarborgd.

De European Data Protection Board (EDPB) bekijkt wat de praktische gevolgen zijn van de uitspraak. En wat eventuele vervolgstappen kunnen zijn. Op korte termijn komt de EDPB met richtlijnen over aanvullende maatregelen die organisaties kunnen opnemen in modelcontracten. De onderhandelingen tussen de VNG met Microsoft over de verwerkersovereenkomst – waar ook de verwerking voor de gemeente Nijmegen onder valt- zijn nog steeds gaande en lopen moeizaam. Dit aspect zal daar als complicerende factor in meegenomen worden.

1.4 Tenant

Een belangrijk risicoaspect en punt van aandacht betreft de inrichting van Exchange online bij de iRVN. Deze is namelijk gebaseerd op één tenant voor de hele regio, met alleen lichte autorisatiescheidingen tussen de verschillende gemeentes en de iRVN. Dit is (indirect) te herleiden uit de oprichting van de iRVN. Bij de start van de samenwerking tussen gemeenten op het gebied van ICT-dienstverlening is door de gemeenten het standpunt ingenomen dat sprake is van één domein voor alle gemeenten. Aangezien een Office-365 tenant maar aan één domein verbonden kan zijn, is er voor de inrichting van Exchange online logischerwijs gekozen voor één tenant.

Hier schuilt echter vanuit privacy het risico in dat het technisch mogelijk is om data te verwerken van een andere gemeente binnen dezelfde tenant, ondanks dat gegevens via autorisaties gescheiden zijn van elkaar. Een ander risico-aspect is dat iedere privacybeschermende maatregel regionaal afgestemd moet worden; het beperkt de mogelijkheden voor de verantwoordelijke gegevensverwerkers om maatregelen te nemen.

Het is mogelijk om iedere gemeente een eigen tenant te geven en deze toch centraal door de iRVN te beheren. Naast de extra privacybescherming geeft dit ook meer zekerheid op continuïteit: de actie van andere gemeentes hebben zo geen effect op de (e-mail)omgeving van de gemeente Nijmegen. Daar tegenover staat dat de kosten voor deze eigen e-mailomgeving fors hoger zullen zijn, aangezien hiervoor ook een eigen Nijmeegs domein van het regionale Karelstad-domein afgescheiden zal moeten worden.

³ <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise/Appendix+2+categories+of+personal+data+and+data+subjects.pdf>

⁴ <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise/DPIA+Office+365+ProPlus+spring+2019+22+July+2019+public+version.pdf>

⁵ <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-data-storage-eu> en <https://msit.powerbi.com/view?r=eyJrJoiYzEyZTc5OTgtNTdlZS00ZTVkLWExN2ItOTM0OWU4NjliOGVjliwidCI6IjcyZjk4OGJmLTg2ZjEtNDZhZi05MWwFILTJkN2NkMDEhZG10NyIsImMiOiV9>

Hoofdstuk 2 Borging rechten van betrokkenen

De AVG kent betrokkenen een groot aantal rechten toe. Hieronder vallen onder meer het recht van inzage, rectificatie en gegevenswissing. Met een overgang naar Exchange online dienen ook de rechten van betrokkenen geborgd te worden.

2.1 Betrokkenen (in de zin van de AVG)

Er zijn twee 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. Anderzijds betreft dit burgers waarover wij (potentieel) persoonsgegevens verwerken in applicaties of op gemeenschappelijke schijven binnen de Exchange omgeving.

2.2 Rechten van betrokkenen

In de huidige omgeving is er in samenwerking met de iRvN een script ontwikkeld om integraal een zoekopdracht uit te kunnen voeren over het merendeel van alle applicaties binnen het Karelstad-domein waarover de dataclassificatie is uitgevoerd. Op deze wijze kan onderzocht worden of een burger en of medewerker voorkomt in applicaties waar persoonsgegevens in verwerkt worden. Hierin schuilt ook gelijk het grootste nadeel; het script kan alleen applicaties doorzoeken, maar niet het gehele Karelstad-domein. Dit betekent dat wij op dit moment slechts gedeeltelijk kunnen voldoen aan de uitvoering van een verzoek op basis van de rechten van betrokkenen. Immers persoonsgegevens die in Outlook of in gemeenschappelijke mappen staan opgeslagen worden nu niet meegenomen.

Exchange online biedt via de Office365-tool; eDiscovery de mogelijkheid om deze zoekopdracht ook voor e-mail te kunnen uitvoeren. Afhankelijk van de licentievorm biedt deze tool beperkte tot uitgebreide mogelijkheden⁶. 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 wat mogelijk nieuwe privacyrisico's opwerpt. De E3-vorm van eDiscovery lijkt daarom afdoende, echter dient deze wel ingericht, voor gebruik door afzonderlijke gemeentes en ingepast te worden in de huidige procedure voor rechten van betrokkenen. Op dit punt is een overgang naar een duurdere E5 licentie dan ook niet nodig.

⁶ <https://www.interlink.com/blog/entry/choosing-the-right-office-365-ediscovery-solution-comparing-e1-vs-e3-vs-e5-plans>

Hoofdstuk 3 Privacydreigingen

Wanneer onderzoeken door het Rijk en privacy-onderzoekers bekijken, zijn een aantal privacy risico's relevant rond de overgang naar Exchange Online en O365. Deze risico's leiden in alle gevallen tot serieuze boetes (tot maximaal 20 miljoen euro) van de Autoriteit Persoonsgegevens indien ze niet opgelost worden.

3.1 Rechten van betrokkenen niet kunnen borgen

Het risico op het niet kunnen borgen van rechten van betrokkenen heeft voor deze situatie de grootste impact. De overstap naar Exchange Online maakt dit risico echter niet groter. Sterker nog, het maakt het mogelijk dat we het risico kunnen verkleinen.

3.2 Onvoldoende privacy by design

Er staat een flinke boete tot maximaal 10 miljoen op het onvoldoende doorvoeren van privacy by design en privacy by default. Het onderstaande schema, op basis van “het blauwe boekje” van Jaap-Henk Hoepman, geeft 8 strategieën die maximaal doorgevoerd moeten worden binnen mogelijkheden en de doelen van de verwerking.



De overstap naar Exchange online zorgt dat e-mailgegevens in grote datacenters van Microsoft komt te staan, wat afdoet aan het scheiden van verwerkingen. Ondanks dat Microsoft maatregelen heeft getroffen om gegevens logisch te scheiden van gegevens andere verantwoordelijken. Ook op gebied van dataminimalisatie ontstaan risico's door overstap naar Exchange online, door de groei van verwerking van diagnostische gegevens. Het gebruik maken van Exchange online binnen één tenant zorgt niet voor een groei van het risico, omdat dit risico al aanwezig is in de huidige omgeving.

3.3 Niet genoeg controle op subverwerkers en verwerkingen

Verschillende onderzoeken naar de gegevensverwerkingen door Microsoft zijn vastgelopen door gebrek aan transparantie door Microsoft. Wel is bekend dat Microsoft diagnostische gegevens ter beschikking stelt aan derden. Inmiddels biedt Microsoft hierover een aantal controlemogelijkheden, maar vanwege het gebrek aan transparantie kan niet met zekerheid gesteld worden dat dit volledige controle biedt.

3.4 Onvoldoende afspraken over verantwoordelijkheden en maatregelen

Het onvoldoende maken en vastleggen van afspraken met andere verwerkers en verantwoordelijken rond een verwerking kan ook leiden tot een boete. Microsoft heeft een aantal contractuele privacygaranties opgenomen in de mantelovereenkomst met de Nederlandse Rijksoverheid. Deze garanties gaan over doelbinding en de mogelijkheid voor de Nederlandse overheid om naleving van deze afspraken te kunnen controleren door effectieve auditrechten. Ook de gewijzigde rol van Microsoft als verwerker voor de meeste Connected Experiences is contractueel vastgelegd.

Microsoft erkent uiteindelijk dat zij als verwerker voor de verwerking van gegevens over het gebruik van Office365 ProPlus, de meeste Connected Experiences en de cloud-opslagdiensten persoonsgegevens verwerkt via de metadata en dat ze deze gegevens maar voor drie toegestane doelen mag verwerken, indien dat proportioneel is. Deze doelen zijn: (1) het technisch aanbieden en verbeteren van de dienst, (2) de dienst up to date houden en (3) het beveiligen van de dienst.

Deze strikte doelbinding geldt zowel voor de inhoudelijke gegevens (Customer Data) als voor alle soorten diagnostische gegevens, inclusief de systeemgegenereerde logboeken van gebeurtenissen op de eigen servers van Microsoft. Microsoft heeft aanvullend gegarandeerd dat zij beide soorten gegevens nooit zal gebruiken voor profilering, data analytics, marktonderzoek of adverteren, tenzij de klant er expliciet om vraagt. Hierbij is specifiek een verbod opgenomen in de overeenkomst op het gebruik van diagnostische gegevens om 'aanbevelingen' te tonen over producten van Microsoft die de klant niet heeft gekocht of niet gebruikt.

Deze afspraken verlagen het risico op onvoldoende privacy by design alleen op het kunnen afdwingen. Door een gezamenlijke aanpak door de Nederlandse overheid zijn de risico's op dit vlak een stuk verlaagd, al blijft er afhankelijkheid van Microsoft die deze partij de macht geeft op bepaalde vlakken onvoldoende mee te werken.

3.5 Overstap naar Exchange Online en DNSSEC, DANE

De overstap naar de cloud met Exchange Online zorgt voor extra risico's op gebied van beveiliging. Hoewel de beveiliging van de datacenters van Microsoft ook binnen de E3 licentie in de basis in orde is, dienen extra maatregelen genomen te worden om grip te houden op de beveiliging van gegevens.

De overgang naar Exchange online heeft geen gevolgen voor de beveiligingsstandaarden, DNSSEC en DANE zoals gebruikt wordt voor Suwinet mail. Deze standaarden, die ook onderdeel van de Baseline Informatiebeveiliging Overheid (BIO) zijn, geven zekerheid over de identiteit van de ontvangende mailserver en voorkomen zo dat aanvallers mailverkeer kunnen 'afluisteren' of aanpassen. Daarnaast dwingt DANE het gebruik van een versleutelde verbinding af. De IRvN routeert de mail op dit moment via KPN (GemNet) en daar worden deze standaarden op toegepast. Wanneer de mail routeert via Microsoft, zouden deze standaarden op dit moment níet toegepast worden. Microsoft is voornemens de standaarden te implementeren (voor inkomende mail in 2021 en voor uitgaande mail al in 2020) maar voor de IRvN, betekent dit dat zij de mail voorlopig via KPN blijven routeren om te voorkomen dat beveiligingsstandaarden die er nu wel zijn, ingeleverd moeten worden. Pas wanneer Microsoft deze beveiligingsstandaarden ondersteunt, zal er worden overgestapt.

Hoofdstuk 4 Risicomitigatie en vertaling naar Nijmeegse situatie

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 het voorgaande hoofdstuk beschreven zijn. Op basis daarvan worden 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).

	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

De dreigingen uit het vorige hoofdstuk hebben allen een lage waarschijnlijkheid, enerzijds door maatregelen die Microsoft al genomen heeft, anderzijds doordat het grootste risico-aspect is dat de Autoriteit Persoonsgegevens daadwerkelijk een onderzoek gaat uitvoeren.

Privacyrisico (dreiging)	Score waarschijnlijkheid	Score impact	Risicoscore
1. Rechten van betrokkenen kunnen niet voldaan worden	3	5	15
2. Onvoldoende beveiliging	2	5	10
3. Onvoldoende privacy by design	1	5	5
4. Niet genoeg controle op subverwerkers en verwerkingen	1	5	5
5. Onvoldoende afspraken over verantwoordelijkheden en maatregelen	1	5	5

In het volgende schema worden de aanbevolen maatregelen per privacyrisico beschreven:

Privacyrisico (dreiging) <i>Kleur conform risicoscore</i>	Aanbevolen maatregel(en)	Effect van maatregel	Impact maatregel op organisatie	Toelichting
1. Rechten van betrokkenen kunnen niet voldaan worden	a. eDiscovery na overgang binnen E3 gebruiken voor aanvragen mbt rechten van betrokkenen	Groot	Beperkt	In beperkte vorm mogelijk binnen de E3-licentie via de eDiscoverytool. Deze moet wel ingericht worden en ingepast in het werkproces.
2. Onvoldoende beveiliging	a. Gebruik multifactor authenticatie	Groot	Beperkt	Dit wordt standaard toegepast door IRVN, maar levert wel een wijziging op ten opzichte van de huidige werkwijze voor de medewerkers van de gemeente Nijmegen.
	b. Stel eisen te stellen aan een account en/of een apparaat voordat toegang tot Office365 services mogelijk is	Groot	Geen	Dit wordt standaard toegepast door IRVN
	c. Mail blijven routeren via KPN voor gebruik Suwinet mail en toepassing beveiligingsstandaarden.	Groot	Geen	Microsoft biedt nu geen beveiligingsstandaard DNSSEC en DANE aan terwijl dit wel is vereist. De huidige routing van de mail via KPN lost dit op.
	d. Aanvullende technische maatregelen gebruik Zorgmail	Groot	Geen	Een aparte en beschikbare plug-in nodig.
3. Onvoldoende privacy by design	a. Verbiedt centraal het gebruik van de Controller Connected Experiences	Beperkt	Groot	Een aantal privacybeschermende tools kan niet meer gebruikt worden, zoals information rights management of gevoeligheidlabels. Een aantal activiteiten levert foutmeldingen op, zoals het openen van een Word-document.
	b. Zet de telemetrie op het niveau 'Neither'	Groot	Geen	Dit wordt al standaard toegepast door IRVN.
	c. Zet het telemetrieniveau in Windows 10 Enterprise op Security (Beveiliging)	Groot	Geen	Binnen de device restrictions instellingen binnen Intune is deze optie geactiveerd. Voor de Windows Specials is een policy object actief.
	d. Schakel het Customer Experience Improvement Programma (CEIP) uit	Groot	Geen	Binnen de configuratie van Microsoft365 Apps voor bedrijven is deze optie geconfigureerd.
	e. Gebruik Customer Lockbox en Customer Key, afhankelijk van de gevoeligheid van de inhoudelijke gegevens	Beperkt	Groot	Hiervoor is de veel duurdere E5-licentie nodig.
	f. Scheidt tenants in de regio of creëer een eigen tenant voor de gemeente Nijmegen	Groot	Groot	Hiervoor is het nodig dat het Karelstad-domein ook gescheiden wordt in meerdere gemeente domeinen, wat ook een migratie inhoudt van alle accounts, apps en data.
	g. Blokkeer het synchroniseren van activiteiten van gebruikers door middel van de "Timeline" functionaliteit	Beperkt	Geen	Binnen de device restrictions instellingen binnen Intune is deze optie geactiveerd. Voor de Windows Specials is een policy object actief.

Privacyrisico (dreiging) <i>Kleur conform risicoscore</i>	Aanbevolen maatregel(en)	Effect van maatregel	Impact maatregel op organisatie	Toelichting
4. Niet genoeg controle op subverwerkers en verwerkingen	a. Zet LinkedIn-integratie uit voor Microsoft werknemer accounts	Groot	Geen	Binnen de configuratie van Microsoft365 Apps voor bedrijven is deze optie geconfigureerd.
5. Onvoldoende afspraken over verantwoordelijkheden en maatregelen	a. Upgrade naar versie 1905 of hoger van Office 365 ProPlus	Groot	Geen	IRVN update de O365-omgeving 2x per jaar.
	b. Actualiseer het bestaande werknemers privacybeleid met specifieke informatie voor welke doelen en onder welke omstandigheden de organisatie de verschillende soorten diagnostische gegevens uit Microsofts verschillende diensten en producten mag bekijken	Groot	Beperkt	Een aanpassing van het privacybeleid.
	c. 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	Beperkt	Beperkt	Workplace Analytics and Activity Reports worden niet gebruikt.
	d. 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	Beperkt	Beperkt	Een aanpassing van het privacybeleid.

Hoofdstuk 5: te nemen maatregelen

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.

Privacyrisico	Effect maatregel op privacyrisico	Impact maatregel op organisatie	Advies
Hoog	Beperkt	Beperkt	Noodzakelijk
Hoog	Beperkt	Geen	Noodzakelijk
Hoog	Beperkt	Groot	Aanbeveling
Hoog	Groot	Beperkt	Noodzakelijk
Hoog	Groot	Geen	Noodzakelijk
Hoog	Groot	Groot	Aanbeveling
Midden	Beperkt	Beperkt	Aanbeveling
Midden	Beperkt	Geen	Aanbeveling
Midden	Beperkt	Groot	Niet noodzakelijk
Midden	Groot	Beperkt	Noodzakelijk
Midden	Groot	Geen	Noodzakelijk
Midden	Groot	Groot	Aanbeveling
Laag	Beperkt	Beperkt	Niet noodzakelijk
Laag	Beperkt	Geen	Niet noodzakelijk
Laag	Beperkt	Groot	Niet noodzakelijk
Laag	Groot	Beperkt	Aanbeveling
Laag	Groot	Geen	Aanbeveling
Laag	Groot	Groot	Niet noodzakelijk

Hieronder staan de te adviseren maatregelen uitgesplitst in 'noodzakelijk', 'aan te bevelen' en 'niet noodzakelijk' aan de hand van de 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. Hierbij worden de volgende maatregelen voorgesteld ter mitigatie van de privacyrisico's.

5.1 Noodzakelijke maatregelen

Noodzakelijke maatregelen zijn maatregelen die aanbevolen worden voor hoge en middelhoge privacyrisico's, waarbij gekeken is naar de balans tussen het effect van de maatregel op het risico en de impact van de maatregel op de organisatie. Voor verdere uitleg is het overzicht privacyrisico's en aanbevolen maatregelen te gebruiken.

- 1a. eDiscovery binnen de E3 licentie gebruiken voor aanvragen mbt rechten van betrokkenen;
- 2a. Gebruik multifactor authenticatie;
- 2b. Stel eisen te stellen aan een account en/of een apparaat voordat toegang tot Office365 services mogelijk is;
- 2c. Mail blijven routeren via KPN voor gebruik Suwinet mail en toepassing beveiligingsstandaarden;
- 2d. Aanvullende technische maatregelen gebruik Zorgmail.

5.2 Aan te bevelen maatregelen

Wanneer de in algemene zin aanbevolen maatregelen een groot effect hebben op een privacyrisico dat an sich niet laag is en de maatregel een beperkte impact heeft op de organisatie, dan wordt deze ook voor de Nijmeegse situatie aanbevolen.

- 3b. Zet de telemetrie op het niveau 'Neither';
- 3c. Zet het telemetrieniveau in Windows 10 Enterprise op Security (Beveiliging);
- 3d. Schakel het Customer Experience Improvement Programma (CEIP) uit;
- 4a. Zet LinkedIn-integratie uit voor Microsoft werknemer accounts;
- 5a. Upgrade naar versie 1905 of hoger van Office 365 ProPlus;
- 5b. Actualiseer het bestaande werknemers privacybeleid .

5.3 Niet-noodzakelijke maatregelen

Wat over blijft zijn maatregelen die vooral lage risico's mitigeren en waar het effect op dat risico ook nog eens beperkt zijn, of waarbij het effect van de maatregel groot is, maar de impact op de organisatie qua kosten en inzet ook.

- 3a. Verbiedt centraal het gebruik van de Controller Connected Experiences;
- 3e. Gebruik Customer Lockbox en Customer Key, afhankelijk van de gevoeligheid van de inhoudelijke gegevens;
- 3f. Scheidt tenants in de regio of creëer een eigen tenant voor de gemeente Nijmegen;
- 3g. Blokkeer het synchroniseren van activiteiten van gebruikers door middel van de "Timeline" functionaliteit;
- 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;
- 5d. Stel beleid op om werknemers te waarschuwen dat zij de mobiele Office apps en de Controller Connected Experiences niet mogen gebruiken, totdat de risico's zijn gemitigeerd.

Hoofdstuk 6 Advies Functionaris voor Gegevensbescherming

Naam Functionaris Gegevensbescherming: Peter Kluver

Contactgegevens: p.kluver@Nijmegen.nl

Datum:

DPIA Oordeel FG gemeente Nijmegen

DPIA: Exchange Online

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA "Exchange Online".

Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA's in het algemeen. In deze wordt oordeel en het daarmee gepaard gaande advies van de opgestelde DPIA weer aan een (meta) oordeel onderworpen. Dat betekent dat niet de diepte ingegaan wordt over de te nemen maatregelen, maar wél of er maatregelen genomen worden, op welk oordeel deze gebaseerd zijn én of oordeelsvorming en genomen maatregelen voorzien zijn van deugdelijke argumentatie.

Uiteindelijk uit zich dit in een eindoordeel die weergeeft of m.i. het gehele voorstel van maatregelen én te nemen maatregelen bij geconstateerde risico's ter verlaging van die risico's (risicomitigatie), te samen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

Op basis van de DPIA versie 1.0 is een eerste scan gemaakt. Dit heeft geleidt tot een aantal op- en aanmerkingen die inmiddels verwerkt zijn in een nieuwe DPIA versie 1.1.3. Deze laatste vormt de onderlegger voor deze toetsing.

Oordeel matrix

De oordeelmatrix is opgebouwd uit een viertal invalshoeken.

De hieronder gehanteerde invalshoeken zijn

- Zijn er reeds DPIA's op dit onderwerp uitgevoerd. En wat zijn daarvan de conclusies?
- Ethisch / politiek bestuurlijke vraag
- Juridische scan (dit betreft meerdere vragen)
- De geconstateerde risico's en voorgestelde maatregelen

Vraag	Argumentatie /	Oordeel
1. Zijn er reeds DPIA's op dit onderwerp uitgevoerd?	Ja, Er is op Rijksniveau een DPIA uitgevoerd	Hier zijn een aantal privacy-risico's uitgekomen die op het niveau Rijk/VNG – Microsoft opgepakt worden. Nijmegen is in die zin onderdeel van de zijde van Rijk/VNG. Wij beschouwen hier de risico's die mogelijkwerwijs optreden door de overgang van Exchange on premises naar Exchange Online.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Het doel is met name vanuit bedrijfsvoeringsmotieven ingezet: <ul style="list-style-type: none"> - Verbetering continuïteit - Verbetering toegankelijkheid - Verbetering uitvoering door IRvN - Gelijktrekken werkwijze vanuit de regio. 	Het verbeteren van de continuïteit en toegankelijkheid zijn valide argumenten.
3. Juridische toets <ul style="list-style-type: none"> a. Doel / grondslag b. Proportionaliteit (1.) c. Subsidiariteit (2.) d. Persoonsgegevens buiten de EER gebruikt? e. Andere partijen betrokken? (verwerkers / subverwerkers)? f. Hoe lang worden gegevens bewaard en termijn en wijze van vernietiging g. Hoe worden gegevens beveiligd 	<ul style="list-style-type: none"> a. Doel is duidelijk. Zie ad. 2. b. Wordt niet expliciet op ingegaan. c. Wordt niet expliciet op ingegaan. d. Ja, zie DPIA Rijk over Exchange Het verwerken buiten de EER heeft aandacht vanuit Europa (European Data Protection Board). Hier worden op dát niveau acties op ondernomen. e. Microsoft. Op- en aanmerkingen in deze liggen in het verlengde van ad 3d. f. Wordt niet expliciet op ingegaan g. Wordt niet expliciet op ingegaan 	<ul style="list-style-type: none"> a. Akkoord. b. Het doel van de overgang wordt wél beschreven. Deze is proportioneel c. Voor zover bekend zijn er geen alternatieven. d. Deze situatie verandert niet door deze overgang. e. Deze situatie verandert niet door deze overgang. f. Deze situatie verandert niet door deze overgang. g. Deze situatie verandert niet door deze overgang. <p>NB. 3f. en 3g. worden wél beïnvloed door de "tenant" die we nu hanteren. Hieronder herhaal ik de tekst uit de DPIA. Mijn advies zal zijn om wel degelijk elke gemeente een eigen tenant te geven. Dit verhoogt de beveiliging op het niveau van aspecten 3f. en 3g. vanuit privacy-overwegingen. Over de financiële effecten hiervan kan ik geen uitspraak doen (staan ook niet vermeld).</p>

4. Risico's en voorgestelde maatregelen	<p>Risico's zijn benoemd.</p> <p>Tabel onder hoofdstuk 4. van de DPIA is helder en duidelijk verwoord en goed navolgbaar.</p> <p>Ook de te nemen maatregelen sluiten daar goed op aan.</p> <p>Mijn advies is om maatregel 3.f. nog nader te beoordelen omdat deze vanuit privacy-overwegingen meer garantie biedt.</p>	<p>Akkoord, mits maatregelen opgevolgd worden.</p> <p>Mijn advies is om maatregel 3.f. te verplaatsen van "niet-noodzakelijke maatregelen" naar "aan te bevelen maatregelen."</p>
---	--	---

1. Het proportionaliteitsvereiste brengt met zich dat het doel van de verwerking van de persoonsgegevens in verhouding moet staan tot de inbreuk op de privacy van de betrokkene.
2. Op basis van het subsidiariteitsvereiste moet altijd gekeken worden of het beoogde doel dat voor de verwerking is vastgesteld, ook op een minder ingrijpende manier en / of met minder ingrijpende middelen kan worden bereikt.

Uit de DPIA:

Tenant

Een belangrijk risicoaspect en punt van aandacht betreft de inrichting van Exchange online bij de IRVN. Deze is namelijk gebaseerd op één tenant voor de hele regio, met alleen lichte autorisatiescheidingen tussen de verschillende gemeentes en de iRvN.

Hier schuilt echter vanuit privacy het risico in dat het technisch mogelijk is om data te verwerken van een andere gemeente binnen dezelfde tenant, ondanks dat gegevens via autorisaties gescheiden zijn van elkaar. Een ander risico-aspect is dat iedere privacybeschermende maatregel regionaal afgestemd moet worden; het beperkt de mogelijkheden voor de verantwoordelijke gegevensverwerkers om maatregelen te nemen.

Het is mogelijk om iedere gemeente een eigen tenant te geven en deze toch centraal door de iRvN te beheren. Naast de extra privacybescherming geeft dit ook meer zekerheid op continuïteit: de actie van andere gemeentes hebben zo geen effect op de (e-mail)omgeving van de gemeente Nijmegen. Daar tegenover staat dat de kosten voor deze eigen e-mailomgeving fors hoger zullen zijn, aangezien hiervoor ook een eigen Nijmeegs domein van het regionale Karelstad-domein afgescheiden zal moeten worden.

Eindoordeel

In dit onderdeel geef ik aan welke maatregelen genomen moeten worden. Welke attentiepunten er zijn bij de uitvoering van dit project. De mate waarin risico's onderkend zijn, afgedekt worden door maatregelen en welk oordeel ik daarover heb. Dat oordeel betreft de risico's die overblijven na handeling: zijn deze te kwalificeren als "hoog", "middel" of "laag"? met als eindoordeel is dit m.i. "aanvaardbaar" of "niet-aanvaardbaar".

Gelet op de genoemde maatregelen beschreven in hoofdstuk 4. van de DPIA versie 1.1.3. en de voorgestelde noodzakelijke uit te voeren maatregelen beschreven in hoofdstuk 5. van de DPIA versie 1.1.3., adviseer ik positief. De resterende risico's na uitvoering van deze maatregelen zijn m.i. "aanvaardbaar".

Dit onder de voorwaarde dat alle noodzakelijke maatregelen in hoofdstuk 5. benoemd ook *minimaal doorgevoerd* moeten worden om de geconstateerde risico's af te dekken.

Ik adviseer *daarnaast* om maatregel 3.f. "scheidt tenants: creëer een eigen tenant voor de gemeente Nijmegen" nog nadrukkelijk te bezien met als doel deze tóch uit te voeren, omdat m.i. de privacy risico's daarmee verlaagd worden.

Concluderend:

Het algeheel beeld is m.i. dat de overgang ten opzichte van de huidige situatie een laag privacy-risico met zich meebrengt.

Om deze reden zie ik geen noodzaak om een voorafgaande raadpleging te hebben met de Autoriteit Persoonsgegevens.

PK/161020.

5.1.2e

06/07/21

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, 4, 19