Ministerie van Justitie en Veiligheid

Samenvatting bij assurancerapportage over profiling-beperkingen bij gebruik van Microsoft's Office 365 ProPlus

1 juli 2020 tot en met 30 september 2020

Building a better working world

VERTROUWELIJK
Ministerie van Justitie en Veiligheid
T.a.v. de heer P.J.G. van den Berg
Postbus 20301
2500 EH DEN HAAG

Den Haag, 17 maart 2021 REQ5267448-C/DW/ib

Samenvatting bij assurance-rapportage over profiling-beperkingen bij gebruik van Microsoft's Office 365 ProPlus

Geachte heer Van den Berg,

U heeft ons gevraagd een audit uit te voeren naar de mate van dataprotectie van persoonsgegevens bij Microsoft, betreffende de wijze waarop Microsoft er voor zorgt dat profilering van persoonsgegevens wordt voorkomen. Conform ons voorstel van 4 december 2019 met kenmerk 1010034055 hebben wij deze audit uitgevoerd.

Bijgaand treft u de samenvatting aan van onze assurance-rapportage conform de NOREA Richtlijn 3000A met het kenmerk REQ5267448-A/DW/ib van 17 maart 2021. Deze samenvatting bevat zodoende dan ook niet alle informatie die in het assurance-rapportage is opgenomen, het lezen van de samenvatting kan dan ook het kennisnemen van het gehele assurance-rapportage niet vervangen.

Onze assurancerapportage is conform uw verzoek Engelstalig opgesteld. In de bijlage ontvangt u onze Nederlandse samenvatting, met daarin de door ons uitgevoerde werkzaamheden en de belangrijkste constateringen.

Verder merken wij op dat in het kader van hoor en wederhoor onze constateringen op 18 februari 2021 met Microsoft zijn afgestemd.

Graag zijn wij bereid tot het geven van een nadere mondelinge toelichting.

Met vriendelijke groet,
Ernst & Young Accountants LLP

w.g. drs. M.M.J.M. (Marc) Welters RE RA
Partner

Introductie

Dit is een samenvatting van de uitgevoerde werkzaamheden naar aanleiding van de assurance-rapportage met betrekking tot verboden profilering van persoonsgegevens in Office 365 ProPlus gedateerd 17 maart 2021 met het kenmerk REQ5267448-A/DW/ib, in opdracht van het Ministerie van Justitie en Veiligheid. Deze samenvatting bevat niet alle informatie die in het assurance-rapport is opgenomen. Derhalve vervangt deze samenvatting dan ook niet de assurance-rapportage.

Wij hebben ons onderzoek verricht in overeenstemming met het Nederlands recht en de Nederlandse Richtlijn 3000A 'Assurance-opdrachten door IT-auditors (attest-opdrachten)' zoals uitgegeven door de beroepsvereniging voor IT-auditors in Nederland (NOREA) en in overeenstemming met International Standard on Assurance Engagements 3000 (herzien), 'Assurance Engagements Other than Audits or Reviews of Historical Financial Information', uitgegeven door de International Auditing and Assurance Standards Board. Deze opdracht is gericht op het verkrijgen van een redelijke mate van zekerheid. Onze verantwoordelijkheden in dit verband worden verder beschreven in het deel 'Verantwoordelijkheden van de IT-auditor' van ons assurance-rapport.

Achtergrond

In februari 2017 ondertekende het Ministerie van Justitie en Veiligheid de Microsoft Business and Services Agreement ("MBSA") met Microsoft voor volumelicenties voor verschillende Microsoft-producten, waaronder Microsoft Office 365 ProPlus. Daarnaast werd in april 2017 overeenstemming bereikt over Amendement 1 van de MBSA, gegeven de aanstaande Algemene Verordening Gegevensbescherming (AVG).

Het Ministerie van Justitie en Veiligheid had reeds verscheidene onderzoeken uitgevoerd of laten uitvoeren naar de verwerking van persoonsgegevens in Microsoft Office 365, te weten:

- Onderzoek door de Autoriteit Persoonsgegevens naar de verwerking van telemetriegegevens bij gebruik van Windows 10 Home en Pro.
- Onderzoek door de afdeling 'Microsoft Rijk Strategic Supplier Management' van het Ministerie van Justitie en Veiligheid naar telemetrie op Windows 10 Enterprise. Dit mede met het oog op de AVG/GDPR die sinds 25 mei 2018 van kracht is.
- Onderzoek de afdeling Microsoft Rijk Strategic Supplier Management naar de verwerking van diagnostische gegevens bij gebruik van Microsoft Office Pro Plus.
- Medio 2019 is wederom onderzoek gedaan naar de verwerking van persoonsgegevens door Microsoft Office 365 ProPlus, nadat Microsoft verbeteringen heeft aangebracht in haar software.

Als resultaat van deze onderzoeken is Amendement 2 op de MBSA overeengekomen met Microsoft Ireland Operations Ltd. Dit om de risico's op het gebied van de bescherming van persoonsgegevens van betrokkenen die de Office 365 ProPlus-producten van Microsoft gebruiken, inclusief cloud services, adequaat te verminderen, en daarmee kan Microsoft 365 ProPlus worden gebruikt door de Nederlandse overheid (DPIA 11 juni 2019, DPIA 22 juli 2019). Ook is een amendement overeengekomen met Microsoft Corporate, aangezien Microsoft Corporate de feitelijke verwerker van diagnostische gegevens is.

Doel van de audit

Het Ministerie van Justitie en Veiligheid heeft bij Microsoft aangekondigd dat een audit zou worden uitgevoerd met betrekking tot het verbod op het verwerken van Klantgegevens en Persoonsgegevens met profilering als doel (zie amendement 2 art. 3).

Op verzoek van het Ministerie is het doel van de door ons uitgevoerde audit als volgt geformuleerd:

Om redelijke zekerheid te bieden dat Microsoft de bescherming van persoonsgegevens in Office 365 ProPlus waarborgt met betrekking tot overeengekomen profileringsbeperkingen, zoals overeengekomen in de overeenkomst (MBSA) en amendementen tussen het Ministerie van Justitie en Veiligheid en Microsoft, gedurende de periode van 1 juli 2020 tot en met 30 september 2020.

Aanpak

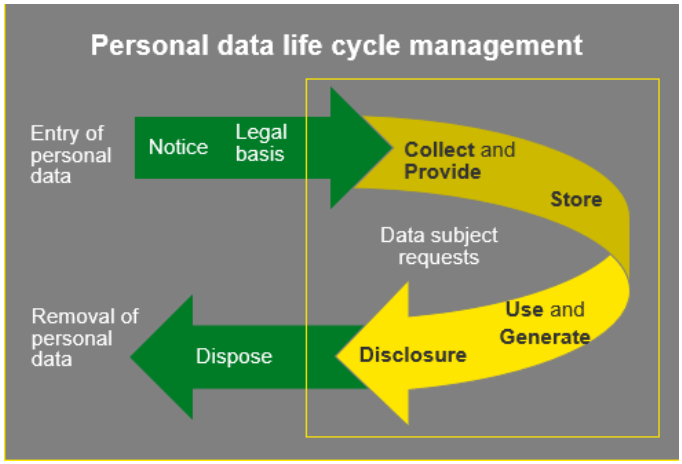
Zoeken naar verboden profilering is als zoeken naar een speld in een hooiberg. Wij hebben voor de aanpak van onze audit overwogen om data-analyses uit te voeren en vervolgens te zoeken naar verboden profilering door Microsoft binnen de infrastructuur van Microsoft. Gezien de omvang en complexiteit van de infrastructuur van Microsoft is gebleken dat het uitvoeren van dergelijke data-analyses, om verboden profilering op te sporen, echter praktisch vrijwel onmogelijk is.

De door ons gekozen aanpak is daarom dan ook gericht op het beoordelen van het toepassen van beheersmaatregelen door Microsoft om te 'voorkomen dat een naald bestaat' (verboden profilering kan voorkomen), en als 'een dergelijke naald zou worden gevonden' (verboden profilering zou worden gedetecteerd), een adequate reactie door Microsoft aanwezig is om 'de naald te verwijderen' (functionaliteit van verboden profilering ongedaan te maken).

Microsoft moet zich voortdurend houden aan de gecontracteerde vereisten betreffende profileringsbeperkingen, zoals overeengekomen in de overeenkomst (MBSA) en amendementen tussen het Ministerie van Justitie en Veiligheid en Microsoft. EY heeft dan ook beoordeeld hoe Microsoft dit bewerkstelligt, zowel qua opzet als werking van beheersmaatregelen. Hiertoe hebben wij eerst, samen met Microsoft, de risico's met betrekking tot verboden profilering in kaart gebracht en vervolgens de beheersmaatregelen geïdentificeerd die nodig zijn om deze risico's te mitigeren. vervolgens is Microsoft verzocht om haar beheersactiviteiten (beleid, procedures en technieken om de risico's te verminderen) inzichtelijk te maken, die zijn getroffen om het risico te beheersen van het niet voldoen aan de gecontracteerde profileringsbeperkingen, en operationeel te blijven voldoen aan de wettelijke en contractuele verplichtingen met betrekking tot de overeengekomen profileringsbeperkingen.

De in kaart gebrachte risico's, criteria en beheersactiviteiten zijn gestructureerd conform de levenscyclus van persoonsgegevens (zie figuur), met een focus op beheersing van het voorkomen van verboden profilering door Microsoft voor de volgende onderdelen:

- De Microsoft-services met betrekking tot het leveren van Office365 ProPlus voor bedrijven op Windows 10 (hierna Office 365 ProPlus);
- Verzamelde, verstrekte en gegenereerde persoonsgegevens gerelateerd aan de Office 365 ProPlus-services.



Figuur – Levenscyclus van persoonsgegevens

De risico's, criteria en beheersactiviteiten hebben betrekking op de volgende onderwerpen:

- Risicobeoordeling van profilering op basis van persoonsgegevens;
- Intern beleid, richtlijnen en instructies om naleving met betrekking tot profilering te waarborgen;
- Ontworpen beheersmaatregelen en effectieve werking van beheersmaatregelen;
- Monitoren, evalueren en rapporteren van compliance;
- Reageren op mogelijke gevallen van niet-naleving.

Wij hebben onderzocht of de beheersmaatregelen daadwerkelijk zijn ontworpen en effectief hebben gewerkt, gedurende de onderzoeksperiode van 1 juli 2020 tot en met 30 september 2020, om de risico's met betrekking tot verboden profilering van persoonsgegevens adequaat te beheersen.

Met de door ons uitgevoerde testwerkzaamheden hebben wij de beheersmaatregelen onderzocht op de in kaart gebrachte risico's, voor zover Microsoft verantwoordelijk was voor de uitvoering van deze beheersmaatregelen. Hiertoe hebben wij per beheersmaatregel de verantwoordelijke voor de desbetreffende maatregel bepaald en hebben wij geïdentificeerd of een beheersmaatregel moet worden uitgevoerd door Microsoft als serviceprovider (verwerker van persoonsgegevens) of door de gebruikersorganisatie (verwerkings-verantwoordelijke voor persoonsgegevens).

Wij hebben geen controleactiviteiten uitgevoerd op beheersmaatregelen waarvoor de gebruikersorganisatie verantwoordelijk is. Wel hebben wij beoordeeld of de geïdentificeerde risico's in voldoende mate worden gemitigeerd door een combinatie van beheersmaatregelen bij Microsoft en de gebruikersorganisatie (Ministerie van Justitie en Veiligheid).

Resultaten

Wij hebben de opzet en de werking van beheersmaatregelen van Microsoft onderzocht binnen de periode van 1 juli 2020 tot en met 30 september 2020. Hierbij hebben wij vastgesteld dat deze beheersmaatregelen effectief zijn om te voldoen aan de beheersdoelstellingen die nodig zijn om met een redelijke waarschijnlijkheid te waarborgen dat geen verboden profilering aanwezig is met betrekking tot Office365 ProPlus, zoals overeengekomen in de overeenkomst (MBSA) en amendementen tussen het Ministerie van Justitie en Veiligheid en Microsoft.

Daarom beschouwen wij de waarschijnlijkheid dat verboden profilering aanwezig is in Office365 ProPlus als laag, en indien toch verboden profilering zou worden opgemerkt, dan zijn beheersmaatregelen aanwezig om dergelijke verboden profilering te elimineren.

Ons oordeel is gevormd op basis van de aangelegenheden zoals deze zijn beschreven in onze assurance-rapportage. De specifiek geteste beheersmaatregelen en de aard, timing en resultaten van die testen staan vermeld in de bijbehorende bijlage 1 (onze beschrijving van testen en resultaten) van de assurance-rapportage.

Beheersdoelstellingen en beheersmaatregelen

Om Microsofts profileringsbeperkingen te onderzoeken, betreft de reikwijdte van de relevante auditcriteria en controleactiviteiten drie gebieden:

- Beheersmaatregelen op privacy en profilering.
- Beheersmaatregelen op beveiliging en toegang.
- Beheersmaatregelen op entiteitsniveau.

Omdat het Ministerie van Justitie en Veiligheid EY verzocht om de audit te concentreren op profileringsbeperkingen, hebben we onze IT-auditactiviteiten gericht op privacy- en profileringsmaatregelen. In sommige gevallen beschouwen we beheersmaatregelen op beveiliging en toegangs- of beheersmaatregelen op entiteitsniveau nog steeds als relevant. In deze gevallen verwijzen we naar deze gebieden.

De privacy- en profileringsbeheersmaatregelen zijn gestructureerd in overeenstemming met de levenscyclus van persoonsgegevens (zie figuur). Deze levenscyclus geeft een beeld van persoonsgegevens vanuit het perspectief van de Verwerkingsverantwoordelijke, aangezien het toepassen van de levenscyclus de volledigheid van criteria en beheersmaatregelen ondersteunt.

Als Verwerkingsverantwoordelijke dient de Nederlandse overheid de persoonsgegevens van personen die gebruik maken van Office 365 ProPlus te beschermen. Daartoe dient de Nederlandse overheid, als onderdeel van de uitbesteding aan Microsoft, Microsoft als Verwerker te instrueren ervoor te zorgen dat de combinatie van beheersmaatregelen door de Verwerker en Verwerkings-verantwoordelijke de profileringsrisico's voor individuen tot een acceptabel niveau reduceert.

Houd er rekening mee dat beperkte profilering impliceert dat profilering kan worden toegestaan, bijvoorbeeld:

- bepalen van adoptiepatronen voor functies;
- functieontwerp en beschikbaarheidsbeslissingen, en
- gepersonaliseerde producthulp bieden over de versie van het product die een gebruiker gebruikt, voor zover dit past binnen de schriftelijke instructies die aan Microsoft zijn gegeven en zoals vastgelegd in de MBSA en Amendementen.

Waar Microsoft Verwerker is, is het de rol van de Verwerkingsverantwoordelijke om met eindgebruikers te communiceren (waarvoor Microsoft de Verwerkingsverantwoordelijke de juiste informatie moet verstrekken, anders kan de Verwerkingsverantwoordelijke niet voldoen aan de vereisten voor de bescherming van persoonsgegevens zoals nodig is).

Microsoft heeft beleid en richtlijnen ontworpen en geïmplementeerd (bijv. Data Handling Standard), bedoeld om te bewerkstelligen dat profilering beperkt is, en alleen tot stand kan worden gebracht na goedkeuring via Microsofts werkwijze voor softwareontwikkeling, juridische beoordelingen (inclusief evaluatie van noodzakelijke Kennisgeving en Keuze), en met documentatie en kennisgeving voor de klant (Verwerkingsverantwoordelijke).

Verwachte beheersmaatregelen van de gebruikersorganisatie als voorwaarde voor de audit

Om gebruik te kunnen maken van Office 365 ProPlus verwacht Microsoft dat:

- De gebruikersorganisatie de huidige documentatie voor de functies van de Online Dienst bestudeert en begrijpt en handelt om hun instructies uit te geven of te wijzigen om aan hun vereisten te voldoen.
- De gebruikersorganisatie stelt zich op om kennisgevingen en mededelingen van Microsoft te ontvangen en hier gepast naar te handelen.
- Gebruikersorganisatie begrijpt dat eerdere service-instellingen van kracht blijven totdat deze worden gewijzigd.

Verder verwacht het Nederlandse Ministerie van Justitie en Veiligheid dat op tenant (gebruikers) niveau, zoals gerapporteerd in de DPIA's (Data Privacy Impact Assessments) van het Ministerie, worden geborgd:

- Upgrade naar versie 1905 of hoger voor Microsoft Office 365 ProPlus.
- Diagnostisch (telemetrie) niveau voor Microsoft Office 365 ProPlus ingesteld op Geen van beide.
- Telemetrieniveau voor Windows 10 Enterprise-beveiliging op 'Beveiliging' of blokkeer al het verkeer voor telemetrie.
- Schakel het Customer Experience Improvement Program (CEIP) uit.
- Schakel LinkedIn-integratie uit.
- Gebruik geen Office-apps op mobiele apparaten.
- Schakel het gebruik van Controller Connected Experiences uit.

Naar aanleiding van de uitgevoerde audit constateren wij dat een gebruikersorganisatie (die optreedt als Verwerkingsverantwoordelijke) de risico's met betrekking tot profilering voor een deel zelf dient te beheersen. De volgende maatregelen dienen op het niveau van gebruikersorganisaties te worden getroffen:

- Gebruikersorganisatie voert jaarlijks een risicoanalyse uit met betrekking tot de risico's en geschiktheid van Office 365. Deze risicoanalyse bevat in ieder geval een overzicht van gegevens die door Office 365 kunnen worden verwerkt en aanvullende maatregelen indien nodig.
- Gebruikersorganisatie configureert (beheren van instellingen) en monitort services in lijn met de uitkomst van de risicoanalyse en het organisatiebeleid.
- Gebruikersorganisatie leidt een admin op om de Office 365-gebruikers professioneel te beheren.
- De gebruikersorganisatie identificeert trapsgewijze maatregelen op basis van de uitkomsten van de risicoanalyses. Deze maatregelen worden jaarlijks herzien.
- De gebruikersorganisatie controleert de serviceberichten op wijzigingen in de services die in gebruik zijn en treedt op als er wijzigingen nodig zijn.
- Gebruikersorganisatie configureert beheersmaatregelen om te instrueren welke en hoe services moeten worden geleverd op basis van door Microsoft aangekondigde of afgedwongen wijzigingen.

- Gebruikersorganisatie leidt hun gebruikers op om op gepaste wijze gebruik te maken van Online Diensten op basis van de vereisten waaraan de gebruikersorganisatie onderworpen is.
- Gebruikersorganisatie verzorgt bewustwordingstraining met betrekking tot privacy en het gebruik van services aan de gebruikers van de gebruikersorganisatie die persoonsgegevens verstrekken voor verwerking door Microsoft.

Beperkingen in gebruik en verspreiding

Onze assurance-rapportage en deze samenvatting zijn bestemd voor het Ministerie van Justitie en Veiligheid - Strategic Vendor Management Microsoft (SLM Rijk) en hun gebruikersorganisaties die gebruik hebben gemaakt van Microsoft Office 365 ProPlus in de periode van 1 juli 2020 tot en met 30 september 2020, en die voldoende inzicht hebben om onze assurance-rapportage en onze beschrijving van toetsingswerkzaamheden en resultaten in aanmerking te nemen, tezamen met overige informatie met inbegrip van informatie over interne beheersmaatregelen die door gebruikersorganisaties zelf zijn getroffen en worden uitgevoerd.

Indien en voor zover u op grond van de wet- of regelgeving gehouden bent onze assurance-rapportage en deze samenvatting aan derden (waaronder de leden van de Tweede Kamer) te openbaren, of indien het u anderszins is toegestaan ons rapport te openbaren, dan dient u het rapport als geheel te openbaren en niet in delen. Bijgevolg dient u, als u de assurance-rapportage en de samenvatting aan derden openbaart, deze derden erop te wijzen dat zij de assurance-rapportage en de samenvatting in zijn geheel dienen te beschouwen.