Ministerie van Justitie en Veiligheid

CIO Rijk, CIO-beraad, CTO-raad, deelnemers SLM MIcrosoft, Google en AWS Rijk, geinteresseerden

Directie Informatievoorziening en Inkoop

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon
Henrique Barnard

T 070 370 79 11

Datum
28 februari 2022

Projectnaam
Strategisch Leveranciersmanagement Microsoft, Google Cloud en AWS Rijk

Ons kenmerk
3867538

memo

Toelichting op de verwerking van bijzondere persoonsgegevens i.v.b. met het hoge risico zoals geïdentificeerd in DPIA op Microsoft Teams

Op 21 februari 2022 heeft Strategisch Leveranciersmanagement Microsoft, Google Cloud en Amazon Web Services (SLM Rijk) de uitkomsten van de gegevensbeschermingseffectbeoordeling (DPIA) op Microsoft Teams, OneDrive en SharePoint Online openbaar gemaakt.

Op sommige plaatsen is een vertekend beeld ontstaan over het geconstateerde hoge risico, dat optreedt bij de verwerking van bijzondere persoonsgegevens.

Vandaag publiceren we een uitleg van de Data Transfer Impact Assessment (DTIA)[1], de DTIA[2] zelf en een door Greenberg Traurig uitgebracht advies[3] met betrekking tot de aanbevelingen van de European Data Protection Board (EDPB)

Om verwerkingsverantwoordelijken verder te helpen bij het duiden van de resultaten van de DPIA en DTIA leggen we hieronder de regels over de verwerking van bijzondere persoonsgegevens uit.

Algemeen: verwerking van bijzondere persoonsgegevens

Het uitgangspunt moet zijn dat organisaties géén bijzondere persoonsgegevens uitwisselen in Teams, of opslaan in SharePoint en OneDrive. Dat mag alleen als ze een beroep kunnen doen op een uitzondering op het verwerkingsverbod in artikel 9 van de AVG (zoals nader ingevuld in de artikelen 22 tot en met 30 uit de UAVG), en een grondslag hebben voor de verwerking als bedoeld in artikel 6 van de AVG.

De twee meest voor de hand liggende uitzonderingen zijn:

1. de uitdrukkelijke toestemming van de betrokkene (voor bijvoorbeeld een juridisch consult, of voor de warme overdracht tussen

[1] Explanation - DTIA on MS Teams, SharePoint and OneDrive

[2] 7 pdf files starting with 'DTIA Dutch government - Teams OneDrive SharePoint 25 Feb 2022 v3' representing various sheets from the excel file

[3] Dutch Ministry of Justice - step 3 EDPB - US

overheidsinstellingen van gezondheidsgegevens in een Teams casus-overleg), en
2. de noodzaak om resultaten van wetenschappelijk onderzoek te kunnen bespreken met vakgenoten wereldwijd

De afweging of een organisatie wel bijzondere persoonsgegevens mag verwerken gaat vooraf aan de risico-afweging over de doorgifte van bijzondere persoonsgegevens via een clouddienst zoals Teams, OneDrive of SharePoint Online. SLM Rijk kan niet alle situaties en omstandigheden voorzien waarin organisaties mogelijk bijzondere persoonsgegevens moeten verwerken of willen uitwisselen. SLM Rijk stelt paraplu DPIA's op, maar de organisaties moeten zelf in kaart brengen of hun gegevensverwerkingen rechtmatig zijn, en of ze die bijzondere persoonsgegevens dus überhaupt mogen verzamelen en delen.

Specifiek: uitwisselen van bijzondere persoonsgegevens in Teams

Het is niet de bedoeling om ziektelijstjes of roddels over bijzondere kenmerken van mensen uit te wisselen in Teams, maar dat mag ook niet op het prikbord in de kantine, en ook niet in e-mails aan alle leden van een afdeling. Er verandert dus niet zo heel veel.

Het kan voorkomen dat er gezondheids- of geloofskenmerken zichtbaar zijn van deelnemers aan een Teams-overleg. Dat betekent niet dat het meteen een verwerking is van bijzondere persoonsgegevens. De Autoriteit Persoonsgegevens past een doelcriterium toe bij de uitleg wanneer foto's bijzondere persoonsgegevens zijn. Kort samengevat: als het niet de bedoeling is om onderscheid te maken naar bijzondere kenmerken, zijn het géén bijzondere persoonsgegevens.

De AP schrijft op
https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/foto-en-film/beeldmateriaal

Er zijn situaties waarin door het maken en publiceren van foto's of filmpjes bijzondere persoonsgegevens worden verwerkt. Denk hierbij bijvoorbeeld aan:

- *Een restaurant dat erop gericht is om mensen in dienst te hebben met een geestelijke of lichamelijke beperking, dat deze mensen op de foto zet of filmt en dit materiaal gebruikt voor een promotieactie om nieuw personeel aan te trekken.*
- *Een leraar die foto's maakt van een sessie waarin kinderen aan het bidden zijn en deze foto's deelt op de website om aan de buitenwereld te laten zien hoe de school het geloof naleeft.*
- *Een organisator van een evenement die een godsdienstig evenement wil promoten onder gelovigen met fotomateriaal waarop bezoekers herkenbaar in beeld zijn gebracht.*

U verwerkt gewone – en dus géén bijzondere – persoonsgegevens met uw foto's of filmpjes als alle 3 de volgende punten gelden:

- *De foto's of filmpjes zijn niet gericht op bijzondere persoonsgegevens of het maken van onderscheid op basis van deze gegevens.*

- *Het is voor u redelijkerwijs ook niet te voorzien dat iemand onderscheid zal maken op basis van uw foto's of filmpjes.*
- *Het is onvermijdelijk dat u bijzondere persoonsgegevens verwerkt als u de foto's of filmpjes maakt.*

Implementatieadvies:

Om organisaties te helpen deze drie spelregels na te leven geven we de volgende adviezen:

1. Schotel nieuwe of externe deelnemers een pop-up voor met spelregels die de deelnemers moeten accepteren, over de omgang met bijzondere persoonsgegevens. Bijvoorbeeld: deel geen bijzondere persoonsgegevens in de chat, ook niet in bestanden. Zo'n pop-up kan getoond worden via de Azure AD. Dat is de laatste tip bij het eerste hoge risico in de DPIA: *Create a Teams and OneDrive privacy policy for internal users and guest users, set rules for sharing of files and images. Make employees and guest users accept these rules through Terms & Conditions imposed by Azure AD.*
2. Wijs, tenzij het absoluut nodig is dat deelnemers in beeld zijn (voor identificatie bijvoorbeeld), deelnemers voor de meeting op de mogelijkheid om hun camera uit te zetten als zij het vervelend vinden om zichtbaar in beeld te komen.
3. Maak beleid in welke gevallen het toegestaan is om een cloudopname te maken van een vergadering, en bepaal een bewaartermijn: bijvoorbeeld een maximum bewaartermijn van 60 dagen. Hoe korter de bewaartermijn, hoe kleiner de kans dat deze gegevens eventueel kunnen worden opgevraagd door Amerikaanse opsporings- en inlichtingendiensten. Microsoft schrijft op https://docs.microsoft.com/en-us/microsoftteams/cloud-recording dat het volgens haar klanten bijna nooit gebeurt dat opnames ouder dan 60 dagen worden teruggekeken. Microsoft schrijft: "*Customers have provided overwhelming feedback that they want more controls to reduce storage clutter created from Teams meeting recordings, 99% of which, on average, are never rewatched after 60 days.*"
4. Neem bij een opname niet de galerij met deelnemers op, en niet de chats.

Voor alle duidelijkheid: bovenstaande adviezen zijn aanvullend op de adviezen in de DPIA en richten zich specifiek op bijzondere persoonsgegevens.

Tot slot: End-to-end encryptie

Als het toch nodig is om bijzondere persoonsgegevens uit te wisselen via deze clouddiensten moet de organisatie end-to-end-encryptie (E2EE) gebruiken om (de hele kleine kans) uit te sluiten dat de Amerikaanse opsporings- en inlichtingendiensten toegang krijgen tot de data. Die versleuteling-met-eigen-sleutel bestaat voor veelgebruikte bestandssoorten die worden opgeslagen in SharePoint en OneDrive, en voor spontane (niet via Outlook geplande) 1-op-1-Teams gesprekken, maar nog niet voor Teams groepsgesprekken, en niet voor cloud-opnames van Teams-gesprekken. Microsoft gaat wel E2EE ondersteunen voor alle Teams-gesprekken, maar daar is nog geen deadline voor bekend. Als

een organisatie E2EE aanzet, zijn cloud opnames automatisch niet meer mogelijk. De organisatie zou dan een eigen server kunnen inrichten om on premise opnames te bewaren.

Met vriendelijke groet,

Team Strategisch Leveranciersmanagement Microsoft, Google Cloud en Amazon Web Services Rijk

Directie Informatievoorziening en Inkoop

Datum
28 februari 2022

Ons kenmerk
3867538