

Data Protection Impact Assessment (DPIA)

Ms.Teams, OneDrive, Azure AD
Provincie Limburg

Vaststelling

Verwerkingsverantwoordelijke:

Naam: Ir. Ron Helwig, clustermanager Organisatie en Informatie

Advies functionaris voor gegevensbescherming:

Naam: [REDACTED]

Versie: 0.7

Status: vastgesteld

Revisie:

| Versie | Datum | Toelichting |
|--------|------------|---|
| 0.1 | 22-10-2024 | Concept omschrijving voorstel, persoonsgegevens en gegevensverwerkingen. |
| 0.2 | 18-11-2024 | Verwerking feedback en eerste aanzet verwerkingsdoeleinden en betrokken partijen. |
| 0.3 | 17-12-2024 | Opmerkingen verwerkt door [REDACTED] |
| 0.4 | 05-02-2025 | Aanpassingen doorgevoerd door [REDACTED] |
| 0.5 | 17-02-2025 | Format aangepast [REDACTED] en opmerkingen doorgevoerd |
| 0.6 | 11-03-2025 | Aanpassingen n.a.v. overleg in PIT |
| 0.7 | 07-05-2025 | Vastgesteld door MTOI |

Inhoudsopgave

Inleiding 4

Managementsamenvatting 5

1. Voorstel 9
2. Persoonsgegevens 9
3. Gegevensverwerkingen 10
4. Technieken en methoden van de gegevensverwerkingen 11
5. Verwerkingsdoeleinden 11
6. Betrokken partijen 11
7. Belangen bij de gegevensverwerkingen 12
8. Verwerkingslocaties 13
9. Juridisch en beleidsmatig kader 13
10. Bewaartermijnen 13
11. Rechtsgrond 15
12. Bijzondere persoonsgegevens 15
13. Doelbinding 15
14. Noodzaak en evenredigheid 16
15. Rechten van betrokkenen 16
16. Risico's voor betrokkenen 17
17. Maatregelen 19

Ondertekening 21

Inleiding

Microsoft Teams, SharePoint, OneDrive en Azure AD maken deel uit van de samenwerkingsomgeving van Microsoft 365, dat specifiek is ingericht voor gebruik binnen de Provincie Limburg. Deze systemen ondersteunen online samenwerking, veilige gegevensopslag en controle over toegang. Met deze DPIA wordt beoogd een compleet beeld te geven van de privacyrisico's en de AVG-borgingen bij het gebruik van deze tools.

De focus ligt op het identificeren van risico's, beoordelen van mitigerende maatregelen, en het naleven van regels omtrent transparantie, beveiliging en gegevensdeling. De scope is afgestemd op de landelijke RijksDPIA en vertaald naar de specifieke situatie in de Provincie Limburg.

Het is goed aan het begin van deze Data Protection Impact Assessment (DPIA) een duidelijk onderscheid te maken tussen twee belangrijke aspecten:

1. Het gebruikelijke onderwerp van een DPIA: Werden er in de applicatie waarin Limburg gaat werken privacygevoelige gegevens verwerkt en levert dat risico's op? Het antwoord daarop is ja: Limburg zet Teams, SharePoint en OneDrive in voor het faciliteren van 'vrij samenwerken', maar in deze omgevingen wordt ook regelmatig privacygevoelige informatie opgeslagen.
2. Het onderwerp dat veel organisaties die werken in de Microsoft Cloud al langer bezighoudt: Verzamelt Microsoft automatisch privacygevoelige gegevens en levert dat risico's op? Het antwoord is ja: Teams, SharePoint, OneDrive en Azure AD draaien allemaal volledig in de Microsoft Cloud, dus alle informatie die daarin wordt opgeslagen en gedeeld, komt ook in die cloud terecht. Dat zijn heel veel persoonlijke sporen, in elk geval van medewerkers, en levert daarmee de vraag op naar het risico van deze verzameling en verwerking van diagnostische gegevens, dat wil zeggen, gegevens over het individuele gebruik van de diensten.

Deze DPIA van de Provincie combineert deze twee aspecten.

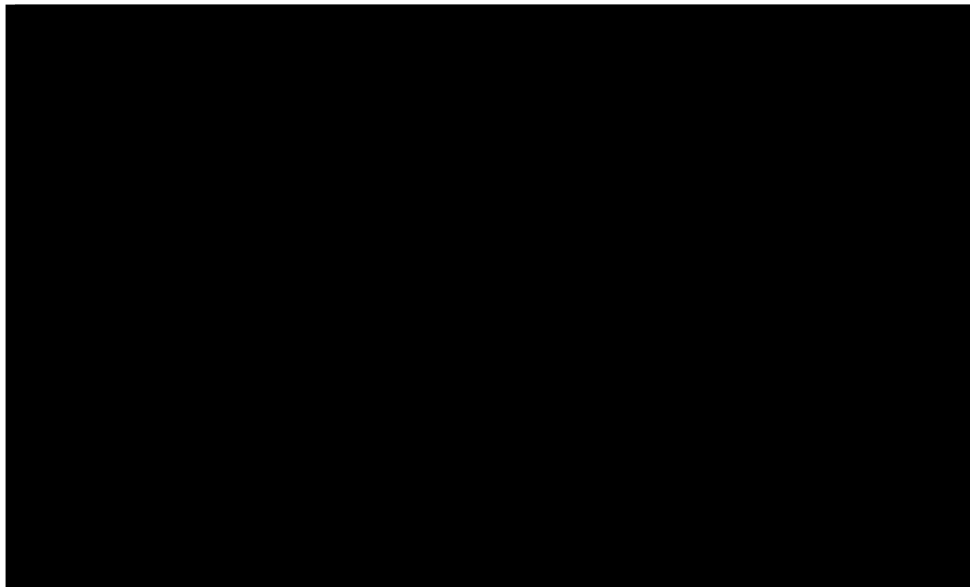
De Provincie Limburg gaat Microsoft Teams (in combinatie met SharePoint, OneDrive en rechtentoeiening vanuit Azure AD) inzetten voor de ondersteuning van 'processen in de vrije samenwerking'. In deze processen zullen officieel weinig privacygevoelige gegevens (zoals klantgegevens) worden opgeslagen, want voor processen waarin klantgegevens een rol spelen, zal een zaakstelsel (als opvolger van [REDACTED]) worden aangeschaft en ingericht.

Niettemin is te verwachten dat regelmatig persoonsgegevens (tijdelijk) zullen landen in deze omgeving, omdat Teams ook de vervanger is van de netwerkschijven. Ook deze netwerkschijven werden gebruikt om klantgegevens (bijvoorbeeld uit de voorbereiding van het vergunningen- of subsidieproces) te 'parkeren' voor later gebruik in de omgeving waarin ze formeel moesten worden opgeslagen, beheerd en gearhiveerd.

Ook zullen (in beperkte mate) gegevens en persoonlijke beleidsopvattingen van medewerkers van de Provincie Limburg in Teams worden opgeslagen die niet zomaar openbaar zijn. Daarbij is het wel goed om te weten dat de Microsoft 365-omgeving sowieso geen openbare omgeving is. Toegang van buiten moet altijd worden gefaciliteerd door een medewerker van de Provincie Limburg.

Er zullen maatregelen worden genomen om te voldoen aan dataclassificatie. Om deze reden – namelijk om alle privacyrisico's in beeld te brengen en tegenmaatregelen te kunnen treffen – wil de Provincie Limburg een DPIA voor Teams, SharePoint en OneDrive uitvoeren.

De DPIA gaat ook over de privacyrisico's van het gebruik van de Microsoft Cloud voor de inhoudelijke gegevens die je via deze diensten kunt delen. De bevindingen, risico's en maatregelen uit de RijksDPIA zijn vertaald naar de Limburgse situatie. De DPIA voor Limburg zal in principe worden geactualiseerd op het moment dat de rijksbrede DPIA wordt geactualiseerd. Azure AD is overigens in deze DPIA alleen in scope als het gaat om authenticatie en autorisatie, het uitdelen van rechten binnen de Microsoft-omgeving.



Bronnen:

- Ministerie van Justitie en Veiligheid/SURF, [DPIA on Microsoft](#) Teams, OneDrive SharePoint and Azure AD (Versie 16 februari 2022).
- Ministerie van Justitie en Veiligheid, [Memo](#) DPIA Microsoft Teams, OneDrive en SharePoint online.
- Microsoft Nederland, [Samenvatting](#)-NL-DPIA-Teams-OneDrive-SharePoint.
- Microsoft, [MS 365 data protection](#) – DPA for 2023.
- Provincie Limburg, Governance vrije samenwerking in Microsoft Teams, 2024.
- [Redacted]

Managementsamenvatting

De Provincie Limburg gebruikt Microsoft Teams, SharePoint, OneDrive en Azure AD in principe niet voor de verwerking van privacygevoelige informatie. Wel komen alle gegevens rond activiteiten van medewerkers en de informatie die ze opslaan en delen binnen Teams, SharePoint, OneDrive en Azure AD in de Microsoft Cloud terecht. De gegevens kunnen worden onderverdeeld in inhoudelijke gegevens (persoons- en werkgerelateerde gegevens) en diagnostische gegevens (technische en analytische gegevens). Ook wordt in Teams regelmatig privacygevoelige informatie geplaatst uit processen die feitelijk niet door Teams worden ondersteund.

De inzet van Microsoft Teams, SharePoint, OneDrive en Azure AD levert de volgende privacyrisico's voor gebruikers, en dus ook voor de Provincie Limburg op:

| No | Risico | Tegenmaatregel |
|----|---|----------------|
| 1. | Gebrek aan helderheid de browser-gebaseerde verzameling van telemetriegegevens en de telemetrie-events over het gebruik van de zogenaamde verbonden ervaringen (Connected Experiences). | [Redacted] |
| 2. | Microsoft kan de gebruikersnaam en/of het e-mailadres van een werknemer verzamelen, samen met de naam van de klant (de tenant) en het bestandspad met de volledige naam van het document. | [Redacted] |
| 3. | Microsoft kan via Teams Analytics & reports een gedetailleerd inzicht bieden over individueel werkgedrag van medewerkers. | [Redacted] |

| | | |
|----|--|------------|
| 4. | Bijzondere persoonsgegevens die niet met een eigen sleutel zijn versleuteld. | [Redacted] |
| 5. | Privacygevoelige informatie wordt opgeslagen in Teams. | [Redacted] |
| 6. | Onrechtmatige toegang tot persoonsgegevens | [Redacted] |
| 7. | Ongewenste wijziging van persoonsgegevens | [Redacted] |

| | | |
|----|------------------------------------|--------------------------|
| | | |
| 8. | Verdwijnen van persoonsgegevens | [REDACTED] [REDACTED] |

[REDACTED]

[REDACTED]

[REDACTED]

Beschrijving van de Kenmerken van Gegevensverwerkingen in Teams en OneDrive

De Provincie Limburg biedt geen individuele Teams-omgevingen aan medewerkers. Teams-sites worden pas beschikbaar gesteld wanneer een Team wordt aangemaakt binnen de organisatiebrede Teams-omgeving ([REDACTED]).

[REDACTED]

Binnen deze DPIA verwijst de term "Teams" naar zowel het Microsoft Teams-platform als de gekoppelde SharePoint-sites.

OneDrive is ingericht als een persoonlijke digitale werkruimte voor de medewerkers van de Provincie Limburg. Deze werkruimte mag uitsluitend worden gebruikt voor zakelijke informatie die (nog) niet mag worden gedeeld met collega's. Het is toegestaan om een beperkte hoeveelheid persoonlijke gegevens op te slaan.

Echter, samenwerken vanuit OneDrive wordt in de governance als oneigenlijk gebruik beschouwd en is daarom niet toegestaan.

De Provincie Limburg hanteert de definitie van een Team (in de Teams-applicatie) als: "een digitale samenwerkingsomgeving voor een specifieke groep personen met een duidelijk omschreven doel." Voorbeelden van deze doelen zijn:

- Samenwerken in een cluster,
- Samenwerken aan een project,
- Samenwerken binnen een proces (langdurige samenwerking).

Volgens de recent opgestelde visie op informatiebeheer en de hiervoor vastgestelde governance, is Teams specifiek bedoeld voor processen die vallen onder vrije samenwerking. Welke processen dit omvat, wordt nader toegelicht in Bijlage 1.

Andere processen worden ondersteund door procesapplicaties of een (nog te selecteren en aan te schaffen) zaakstelsel. Voor deze applicaties wordt een

aparte DPIA opgesteld. Als een zaakstelsel of een van de procesapplicaties SharePoint gebruikt voor documentopslag of dossiervorming, wordt deze gekoppeld aan de DPIA van dat specifieke stelsel

Binnen Teams worden geen processen ondersteund waarin informatie van burgers of bedrijven structureel wordt opgeslagen. Toch kan er onbedoeld of tijdelijk dergelijke informatie in Teams terechtkomen door onwetendheid of gemakzucht. Voor deze situaties zijn maatregelen opgenomen onder de risico's 5 en 6 uit de risicotabel. Daarnaast wordt een kwaliteitscyclus opgezet om oneigenlijk gebruik van Teams en OneDrive zo veel mogelijk te voorkomen. Met behulp van [REDACTED] wordt door het gebruik van een goed afgestemde en deels gestandaardiseerde termenset geïdentificeerd in welke documenten mogelijk privacygevoelige gegevens zijn vastgelegd en welke vervolgstappen nodig zijn.

Als onderdeel van de governance omtrent Teams is opgenomen dat geen bijzondere persoonsgegevens in Teams worden opgeslagen. Dit principe maakt nadrukkelijk onderdeel uit van de implementatie van Teams, de bijbehorende spelregels en trainingen.

Azure Active Directory (Azure AD) speelt een ondersteunende rol door het beheren van de toegangsrechten tot de Microsoft 365-omgeving. Dit stelsel wordt gebruikt om medewerkers veilig en met de juiste machtigingen toegang te geven tot Teams, SharePoint en OneDrive.

Voorgenomen Gegevensverwerkingen

- Verwerking in Teams: De verwerking van privacygevoelige gegevens is formeel niet toegestaan of beperkt tot een minimum. Teams is bedoeld voor vrije samenwerking. Binnen Teams kunnen geclassificeerde bestanden worden opgeslagen die niet per definitie privacygevoelig zijn. Deze bestanden worden beveiligd [REDACTED] om ongewenste toegang te voorkomen. [REDACTED]
- Rol van Azure AD: Binnen deze DPIA is Azure Active Directory (Azure AD) voornamelijk relevant omdat het de authenticatie en toegang van medewerkers tot de Microsoft 365-omgeving regelt.
- Loggegevens: Alle activiteiten binnen de Microsoft 365-omgeving worden gelogd. Deze loggegevens worden gebruikt:
 - Om gebruikerservaringen te verbeteren, zoals het automatisch genereren van een overzicht van recent geopende bestanden.
 - Voor rapportages over het gebruik van de omgeving als geheel (zowel voor interne analyse als voor gebruik door Microsoft zelf).

Beschrijving van de doeleinden van de Verwerkingen

De verwerking van gegevens binnen Teams en OneDrive heeft de volgende doelen:

1. Veilige interne en externe samenwerking: Het stelsel ondersteunt medewerkers bij het delen van informatie en samenwerken op een manier die voldoet aan de gestelde beveiligingseisen.
2. Toegangsbeheer: Het bieden van veilige en gecontroleerde toegang tot Teams, SharePoint en OneDrive via Azure AD.

3. Audittrail: Het vastleggen van activiteiten om na te gaan dat medewerkers doelmatig en rechtmatig werken. Hiermee kan worden voldaan aan eisen van verantwoording en controle.

A. Beschrijving algemene kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

1. Voorstel

Beschrijf het voorstel waar de DPIA op toeziet op en benoem hoe het voorstel tot stand is gekomen en wat de beweegredenen zijn achter de totstandkoming van het voorstel.

De DPIA ziet toe op de verwerking van privacygevoelige en andere vertrouwelijke of zeer vertrouwelijke gegevens in Teams, SharePoint, OneDrive en Azure AD.

2. Persoonsgegevens

Beschrijf alle [persoonsgegevens](#) die worden verwerkt. Classificeer deze persoonsgegevens naar: gewoon, [gevoelig](#), [strafrechtelijk](#) en wettelijk identificatienummer. Geef per categorie [persoonsgegevens](#) aan welke persoonsgegevens worden verzameld en geef aan wat de bron is van deze persoonsgegevens.

| Categorie betrokkenen | Categorie persoonsgegevens | Persoonsgegevens | Type | Bron |
|---------------------------------|---|---|--|------------------------|
| Medewerkers Provincie Limburg | Contactgegevens, handelingen en opvattingen | Naam, zakelijk e-mailadres, opvattingen, authenticatiegegevens, toegangsrechten, audit, log- en toegangsgegevens, | Gewoon | Azure AD en betrokkene |
| Externen (burgers en bedrijven) | Contactgegevens en gegevens over zaken met de Provincie | NAW, opvattingen, gegevens over zaken met de Provincie, e-mailadressen, organisatiegegevens, authenticatiegegevens, toegangsrechten, audit, log- en toegangsgegevens, | Gewoon, gevoelig en mogelijk bijzonder | Betrokkene zelf |

Als Teams op een goede manier wordt gebruikt, volgens de afgesproken governance en spelregels, worden geen privacygevoelige gegevens in Teams opgeslagen. Informatie met een vertrouwelijk karakter wordt beschermd door:

- [REDACTED]
- [REDACTED]
- [REDACTED]

Deze maatregelen, bedoeld voor vertrouwelijke gegevens in het algemeen, zijn ook toepasbaar op privacygevoelige gegevens. Als er meer gegevens worden opgeslagen dan volgens de afgesproken governance, dan bestaat er een kans dat er gevoelige en bijzondere persoonsgegevens worden opgeslagen in Teams.

3. Gegevensverwerkingen

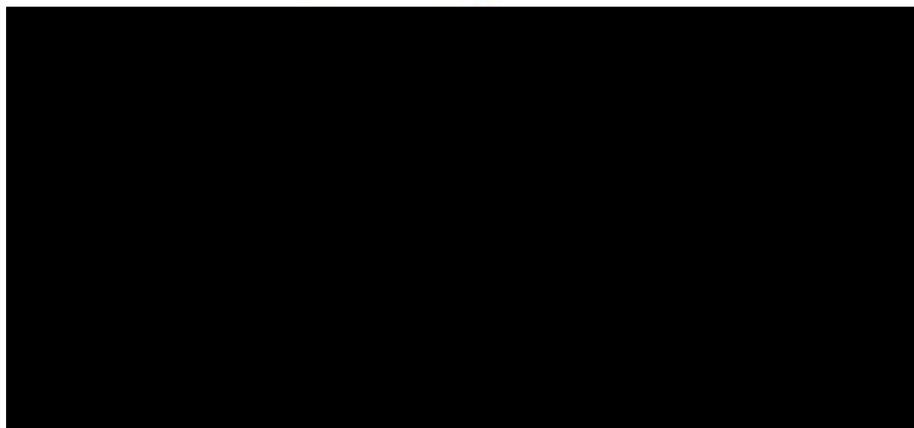
Geef alle [gegevensverwerkingen](#) weer en geef aan welke categorieën persoonsgegevens worden verwerkt per gegevensverwerking. Desgewenst kan een stroomschema van de gegevensverwerkingen worden toegevoegd.

Het kan daarbij gaan om het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van persoonsgegevens.

| Gegevensverwerking | Categorieën persoonsgegevens |
|---|---|
| Inloggen en werken in Teams | Contactgegevens |
| Inhoudelijke informatie opslaan en delen in Teams | Contactgegevens, opvattingen en gegevens over zaken met de Provincie. |
| Audittrail | Contactgegevens medewerkers en handelingen medewerkers |

- In Teams en OneDrive vindt gegevensverwerking zoals bedoeld in de AVG plaats, in veel gevallen zou die gegevensverwerking in andere systemen (procesapplicaties, zaakstelsel) moeten plaatsvinden.
- In Azure AD worden persoonsgegevens verwerkt om personen toegang te geven tot de digitale werkomgeving EN de juiste rechten op de juiste informatie binnen die omgeving.
- In de praktijk zullen soms wel bijzondere en gevoelige persoonsgegevens worden vastgelegd, ook al is dit tegen de governance en de spelregels.
- In de audittrail van Microsoft Teams worden verschillende acties en gebeurtenissen vastgelegd om de activiteiten van gebruikers binnen de applicatie te kunnen volgen en te monitoren. De specifieke informatie die wordt vastgelegd in de audittrail kan onder andere het volgende omvatten:
 - **Gebruikersactiviteit:** acties zoals het aanmaken, bewerken of verwijderen van berichten, kanalen, vergaderingen en bestanden.
 - **Toegangs- en inloginformatie:** Wanneer een gebruiker inlogt op Teams, inclusief het IP-adres en het apparaat dat wordt gebruikt.
 - **Bestandshandelingen:** Wanneer bestanden worden geupload, gedownload, gedeeld of bewerkt binnen Teams.
 - **Vergaderinformatie:** Gegevens over het starten, deelnemen en verlaten van vergaderingen, inclusief details over de deelnemers.

- **Wijzigingen in instellingen:** Wijzigingen in teaminstellingen, lidmaatschapsstatus of machtigingen.
- **Verwijderde berichten:** Berichten die zijn verwijderd door gebruikers of beheerders.
- **Toegang tot externe apps en integraties:** Acties die betrekking hebben op apps of integraties die zijn toegevoegd aan Teams, zoals het openen van een gekoppelde SharePoint-locatie of het gebruiken van een externe tool. Deze gegevens worden opgeslagen in de [REDACTED] die beheerders kunnen raadplegen via het Microsoft 365-beheercentrum ([REDACTED]), waar ze kunnen worden doorzocht en geanalyseerd voor nalevings-, beveiligings- en beheerdoeleinden.



4. Technieken en methoden van de gegevensverwerkingen

Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem, bijvoorbeeld, of sprake is van bijvoorbeeld (semi-) geautomatiseerde besluitvorming, profilering, een cloudoplossing of big data-verwerkingen en, zo ja, beschrijf waaruit dat bestaat.

(Deels) geautomatiseerd:

1. Inhoudelijke gegevens (persoons- en werkgerelateerde gegevens)

Dit zijn gegevens die direct bijdragen aan communicatie en samenwerking binnen Teams:

- Chats, berichten en reacties;
- Privéchats tussen gebruikers;
- Kanaalgesprekken en vergaderchats;
- Reacties op berichten, bestanden en gedeelde documenten;
- Bestanden die worden geüpload in Teams (opgeslagen in OneDrive/SharePoint);
- Versiegeschiedenis van documenten;
- Metadata van documenten (auteur, tijdstempel, wijzigingen);
- Vergaderingen en oproepen;
- Opgenomen vergaderingen (video, audio, gedeeld scherm);
- Automatische transcripten en ondertiteling;
- Deelnamegegevens (wie was aanwezig, hoe lang);

- Gebruikersinformatie en accountgegevens;
- Naam, e-mailadres, profielfoto;
- Teams- en kanaallidmaatschappen;
- Functie en organisatiegegevens (indien gekoppeld aan Azure AD);
- Gegevens uit geïntegreerde apps;
- Taken en berichten uit [REDACTED], enz.;
- Activiteiten in [REDACTED] of andere apps.

2. Diagnostische gegevens (technische en analytische gegevens)

Dit zijn gegevens die Teams verzamelt om prestaties te monitoren, problemen op te lossen en beveiliging te garanderen:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

5. Verwerkingsdoeleinden

Beschrijf de doeleinden van alle gegevensverwerkingen.

Voeg aanvullende informatie toe in het tekstveld.

De verwerkingsdoeleinden: waarom verwerk je persoonsgegevens? In de AVG noemen ze dit het doel en de grondslag. De (wettelijke) basis waarop je persoonsgegevens verwerkt. Er zijn 6 mogelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.

| Gegevensverwerking | Verwerkingsdoeleinde | Oorspronkelijk verwerkingsdoeleinde |
|---|---|-------------------------------------|
| Inloggen en werken in Teams | Autorisatie en authenticatie. Medewerker toegang verlenen tot de Teams-omgeving. | N.v.t. |
| Inhoudelijke informatie opslaan en delen in Teams | Samenwerken | N.v.t. |
| Audittrail | Logging handelingen | N.v.t. |
| | | |

Om te kunnen samenwerken in Teams zijn persoonsgegevens nodig van de medewerkers die werken in Teams.

6. Betrokken partijen

Benoem alle partijen die betrokken zijn en deel deze in per gegevensverwerking. Deel deze partijen in onder de rollen: [verwerkingsverantwoordelijke](#), [gezamenlijke verwerkingsverantwoordelijke](#), [verwerker](#), [sub-verwerker](#), [verstrekker](#), [ontvanger](#), [betrokkene\(n\)](#) en [derde](#). Wanneer bekend, benoem ook welke functionarissen/afdelingen binnen deze partijen toegang krijgen tot welke categorieën persoonsgegevens. Voeg aanvullende informatie toe in het tekstveld.

| Naam partij | Rol partij | Functies/afdelingen | Persoonsgegevens |
|-------------------------------|------------------------------|-----------------------------|---|
| Provincie Limburg | Verwerkingsverantwoordelijke | Gehele organisatie | Naam, zakelijk e-mailadres, opvattingen, authenticatiegegevens, toegangsrechten, audit, log- en toegangsgegevens, |
| Medewerkers Provincie Limburg | Betrokkenen | Gehele organisaties | Naam, zakelijk e-mailadres, opvattingen, authenticatiegegevens, toegangsrechten, audit, log- en toegangsgegevens, |
| Externen | Derden | Alle uitgenodigden externen | NAW, opvattingen, gegevens over zaken met de Provincie, e-mailadressen, organisatiegegevens, authenticatiegegevens, toegangsrechten, audit, log- en toegangsgegevens, |
| Microsoft | Verwerker | - | NAW, opvattingen, telefoonnummers, e-mailadressen, gegevens over zaken met de Provincie Limburg. |

7. Belangen bij de gegevensverwerkingen

Beschrijf alle belangen die de betrokken partijen hebben bij de gegevensverwerkingen. Vraag betrokkenen of hun vertegenwoordigers ook naar hun mening over de verwerking indien relevant. Licht deze mening toe onder het belang van de betrokkenen.

| Betrokken Partij | Belangen |
|-------------------------------|---|
| Provincie Limburg | Medewerkers werken samen in en slaan hun informatie op in een gedeelde omgeving binnen het domein van de organisatie. |
| Medewerkers Provincie Limburg | Medewerkers kunnen makkelijk hun werk doen en laagdrempelig samenwerken op een veilige en verantwoorde manier. |
| Externen | Externen kunnen makkelijk en veilig samenwerken met de organisatie. |
| Microsoft | Levering van de diensten. |

8. Verwerkingslocaties

Deze tabel moet enkel worden ingevuld als de verwerkingslocatie zich buiten de EER bevindt.

Alle gegevensverwerkingen vinden binnen de EER plaats. Microsoft heeft EU Data boundary ingevoerd zodat risico op verplicht doorgeven informatie aan Amerikaanse regering nihil is.

Uit de tussen de Provincie Limburg en Microsoft gesloten Enterprise Agreement volgt dat iedere doorgifte van persoonsgegevens buiten de EER in het kader van de overeenkomst wordt beheerst door de modelcontractbepalingen die door Microsoft zijn opgesteld en gepubliceerd als de Bijlage bescherming van persoonsgegevens voor Producten en Diensten. De Enterprise Agreement stelt dat, indien de modelcontractbepalingen niet langer van toepassing of beschikbaar zijn, Microsoft garandeert dat er een andere passende waarborg voor de doorgifte van persoonsgegevens kan worden aangewezen. Mocht blijken dat de doorgifte van persoonsgegevens desondanks of bij het ontbreken van een passende waarborg niet rechtmatig is, dan geeft de Enterprise Agreement Provincie Limburg de bevoegdheid om het gebruik van Teams/Sharepoint met onmiddellijke ingang te beëindigen.

9. Juridisch en beleidsmatig kader

Benoem alle en beleid met mogelijke gevolgen voor de gegevensverwerkingen. De AVG en de Richtlijn¹ hoeven niet genoemd te worden. Voeg aanvullende informatie toe in het tekstveld.

- Baseline Informatieveiligheid Overheid (2.0).

De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen.

- Bedrijfsimpactanalyse (BIA)

¹ Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

10. Bewaartermijnen

Bepaal de [bewaartermijnen](#) van de persoonsgegevens aan de hand van de gegevensverwerkingen en de verwerkingsdoeleinden. Motiveer waarom deze bewaartermijnen niet langer zijn dan strikt noodzakelijk ten opzichte van de verwerkingsdoeleinden. Beschrijf wie toeziet op de bewaartermijn en de mogelijke vernietiging of archivering aan het einde van de bewaartermijn en de mogelijke vernietiging of archivering aan het einde van de bewaartermijn. Voeg aanvullende informatie toe in het tekstveld.

| Gegevensverwerking | Verwerkingsdoeleinde | Categorie Persoonsgegevens | Bewaartermijn | Motivatie bewaartermijn |
|---|------------------------------|--|---|-------------------------|
| Inloggen en werken in Teams | Authenticatie en autorisatie | Contactgegevens | Duur dienstverband | Centraal beleid |
| Inhoudelijke informatie opslaan en delen in Teams | Samenwerken | Contactgegevens, opvattingen en gegevens over zaken met de Provincie | Zie toelichting. | |
| Audittrail | Logging handelingen | Contactgegevens medewerkers en handelingen medewerkers | <p>De standaard bewaartermijn van de audittrail in Microsoft 365 is 90 dagen.</p> <p>Bij bepaalde abonnementsvormen, zoals Microsoft 365 E5 of met het gebruik van Microsoft 365 Compliance Center, kan de bewaartermijn worden verlengd tot maximaal 1 jaar (365 dagen), afhankelijk van de beheerdersinstellingen.</p> <p>Voor nog langere bewaartermijnen kan gebruik worden gemaakt van Microsoft 365</p> | |

| Gegevens- verwerking | Verwerkings- doeleinde | Categorie Persoons- gegevens | Bewaartermijn | Motivatie bewaar- termijn |
|-------------------------|---------------------------|------------------------------------|--|---------------------------------|
| | | | Advanced Compliance of eDiscovery- functies, waarmee logbestanden meerdere jaren bewaard kunnen blijven. | |

Toelichting

- De bewaartermijnen van bestanden in Teams zijn afhankelijk van het retentielabel op het kanaal waarin ze staan. Een overzicht van retentielabels is beschikbaar: [REDACTED]
- De bewaartermijn van OneDrive-bestanden is: zolang de medewerker een Microsoft-account heeft.
- Op dit moment is geen specifieke bewaartermijn vastgesteld voor Teams-vergaderingen en -opnames. De bewaartermijn van deze bestanden is afhankelijk van de standaardinstellingen binnen de organisatie. Aangezien er momenteel geen retentiebeleid is geconfigureerd, blijven opnames behouden totdat ze handmatig worden verwijderd door een gebruiker.
- De bewaartermijn van kanaalberichten (in een Team) moeten we nog vaststellen.
- De bewaartermijn van chatberichten is gelijk aan die van e-mails, namelijk zeven jaar voor 'gewone' medewerkers en permanent voor zogenaamde 'sleutelfunctionarissen'.

B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel de rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen en rechten van de betrokkene.

11. Rechtsgrond

Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd. Iedere rechtsgrond moet aan bepaalde voorwaarden voldoen, voeg in de toelichting op de rechtsgrond toe hoe aan deze voorwaarden wordt voldaan. Voeg aanvullende informatie toe in het tekstveld.

| Gegevensverwerking | Rechtsgrond | Toelichting op de rechtsgrond |
|---|--|---|
| Inloggen en werken in Teams | Noodzakelijk op grond van het gerechtvaardigd belang | Ten behoeve van de interne bedrijfsvoering. |
| Inhoudelijke informatie opslaan en delen in Teams | Noodzakelijk op grond van het gerechtvaardigd belang | Ten behoeve van de interne bedrijfsvoering |
| Audittrail | Noodzakelijk op grond van het gerechtvaardigd belang | Ten behoeve van de interne bedrijfsvoering |

12. Bijzondere persoonsgegevens

In beginsel worden er geen bijzondere persoonsgegevens in Teams, SharePoint, OneDrive. Slaan medewerkers meer gegevens op dan volgens de afgesproken governance, dan bestaat er een kans dat er gevoelige en/of bijzondere persoonsgegevens worden opgeslagen in Teams, bijvoorbeeld een BSN of politieke gegevens.

13. Doelbinding

Als de persoonsgegevens voor een ander doeleinde worden verwerkt dan het doeleinde waarvoor de persoonsgegevens oorspronkelijk zijn verzameld, beoordeel of deze (nieuwe) verdere verwerking toelaatbaar is op grond van Unie- of lidstaatrechtelijk recht, dan wel is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld. Voeg in het tekstveld de verenigbaarheidstoets en aanvullende informatie toe.

| Gegevensverwerking | Persoonsgegevens | Doeleinde | Oorspronkelijk doeleinde |
|---|--|-----------|--------------------------|
| Inloggen en werken in Teams | Contactgegevens | n.v.t. | n.v.t. |
| Inhoudelijke informatie opslaan en delen in Teams | Contactgegevens, opvattingen en gegevens over zaken met de Provincie | n.v.t. | n.v.t. |
| Audittrail | Contactgegevens medewerkers en handelingen medewerkers | n.v.t. | n.v.t. |

14. Noodzaak en evenredigheid

Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk en evenredig zijn voor het verwezenlijken van de verwerkingsdoeleinden.

Ga hierbij in ieder geval in op:

- Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?
- Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, worden verwezenlijkt?

Inbreuk op persoonlijke levenssfeer is miniem. De voordelen van digitaal samenwerken zijn enorm. De gegevensverwerking is proportioneel.

In beginsel kan samenwerking via een ander systeem. Echter gelet op de manier van samenwerken binnen Microsoft Teams en de in beginsel minimale verwerking van persoonsgegevens binnen Teams, worden de verwerkingsdoeleinden niet op een meer nadelige wijze verwezenlijkt binnen Teams dan in een ander systeem.

15. Rechten van betrokkenen

Beschrijf de procedure waarmee invulling wordt gegeven aan de [rechten van de betrokkenen](#). Als de rechten van de betrokkene worden beperkt, beschrijf op grond van welke wettelijke uitzondering dat is toegestaan.

| Rechten van betrokkene | Procedure ter uitvoering | Beperking op grond van wettelijke uitzondering |
|--|--------------------------------------|--|
| Recht van inzage | Handleiding rechten van betrokkenen. | N.v.t. |
| Recht op rectificatie en aanvulling | Handleiding rechten van betrokkenen. | N.v.t. |
| Recht op vergetelheid | Handleiding rechten van betrokkenen. | N.v.t. |
| Recht op beperking van de verwerking | Handleiding rechten van betrokkenen. | N.v.t. |
| Recht op dataportabiliteit | Handleiding rechten van betrokkenen. | N.v.t. |
| Recht niet onderworpen te worden aan geautomatiseerde besluitvorming | Handleiding rechten van betrokkenen. | N.v.t. |
| Recht om bezwaar te maken | Handleiding rechten van betrokkenen. | N.v.t. |
| Recht op duidelijke informatie | Handleiding rechten van betrokkenen. | N.v.t. |

Het recht van inzage m.b.t. diagnostische gegevens wordt beperkt. Microsoft heeft toegezegd haar inzage-tool voor Diagnostische Gegevens te verbeteren, om beheerders te helpen bij eventuele inzageverzoeken van individuele werknemers. Dit hulpmiddel is momenteel nog moeilijk te gebruiken. Informeer medewerkers over de inzagemogelijkheden via de Data Viewer tool en door een inzageverzoek in te dienen bij de beheerder(s) van de organisatie. Gebruik Microsoft's Data Viewer tool zelf voor inzage in de diagnostische gegevens en

vergelijk de uitkomsten met een eigen analyse van het uitgaande netwerkverkeer uit een test-omgeving.

C. Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de gegevensverwerkingen.

16. Risico's voor betrokkenen

Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Ga hierbij in ieder geval in op:

- welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen, zoals het verbod op discriminatie;
- de oorsprong van deze gevolgen;
- de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;
- de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.

Gebruik voor de inschatting van de kans, impact en het risico de niveaus 'laag', 'gemiddeld' en 'hoog'. De kans wordt bepaald aan de hand van de formule kans x impact. Gebruikmaken van de bijbehorende kleuren is aan te raden. De onderstaande matrix kan worden gebruikt voor het vaststellen van de risico's voor betrokkenen.

| | | Kans | | |
|--------|--------|------|--------|------|
| | | laag | midden | hoog |
| Impact | hoog | laag | hoog | hoog |
| | midden | laag | midden | hoog |
| | laag | laag | laag | laag |

**De bovenstaande risicomatrix is illustratief. Risico's met een lage impact of lage kans worden als laag ingeschat indien het risico niet verder kan worden gemitigeerd. Zo kan bijvoorbeeld de impact van ransomware hoog zijn, maar door het nemen van de juiste technische maatregelen de kans (zeer) laag. Het risico kan dan ten behoeve van de risico-acceptatie als laag beschouwd worden.*

| Beschrijving risico | Kans | Impact | Risico- inschatting |
|--|------|--------|------------------------|
| Doorgifte van privacygevoelige informatie naar de Amerikaanse overheid. | ■ | ■ | ■ |
| Microsoft is niet erg transparant over de browser-gebaseerde verzameling van telemetriegegevens en de telemetrie-events over het gebruik van de zogenaamde verbonden ervaringen (Connected Experiences). | ■ | ■ | ■ |
| Inzage in individueel werkgedrag | ■ | ■ | ■ |
| Bijzondere persoonsgegevens die niet met een eigen sleutel zijn versleuteld. | ■ | ■ | ■ |
| Onrechtmatige toegang tot persoonsgegevens. | ■ | ■ | ■ |
| Ongewenste wijziging van persoonsgegevens | ■ | ■ | ■ |
| Verdwijnen van persoonsgegevens | ■ | ■ | ■ |

De vijf lage gegevensbeschermingsrisico's bij de verwerking van diagnostische hangen samen met de volgende omstandigheden:

1. [Redacted text block containing multiple lines of information]

[illegible][illegible][illegible][illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]


Beschrijf de voorgenomen maatregelen om de hiervoor beschreven risico's van de gegevensverwerkingen voor de vrijheden en rechten van de betrokkenen aan te pakken.

17. Maatregelen

In de OneDrive kunnen gevoelige en bijzondere persoonsgegevens worden beschermd met Microsoft's Double Key Encryption (DKE).

[illegible]

| Risico | Maatregelen | Resterend risico en risico-inschatting | Beheerder van maatregelen |
|--|-------------|--|---------------------------|
| Microsoft is niet erg transparant over de browser-gebaseerde verzameling van telemetriegegevens en de telemetrie-events over het gebruik van de zogenaamde verbonden ervaringen (Connected Experiences). | [REDACTED] | Midden | |
| Inzage in individueel werkgedrag door externe partij. | [REDACTED] | [REDACTED] | |
| Bijzondere persoonsgegevens die niet met een eigen sleutel zijn versleuteld. | [REDACTED] | [REDACTED] | |

| | |
|--------------|--|
| Handtekening |  |
|--------------|--|

Bijlage 1 Processen in de vrije samenwerking
Stand van zaken 19 november 2024
Actuele versie vind je hier: [>>>](#)

| Bedrijfsprocessen | Werkprocessen |
|--------------------|---------------|
| [Redacted content] | |

