DPIA iVRI’s

[Naam wegbeheerder]

[Versie]

**Versiebeheer**

|  |  |  |  |
| --- | --- | --- | --- |
| Versie | Datum | Door | Opmerkingen |
| 0.1 | … | … | … |
| 0.2 |  |  |  |
| 0.3 |  |  |  |
| 0.4 |  |  |  |
| 0.5 |  |  |  |
| 0.6 |  |  |  |
| 0.7 |  |  |  |

**Vertrouwelijkheidsniveau**

[Openbaar / bedrijfsvertrouwelijk / geheim]

# Samenvatting

[optioneel]

Inhoudsopgave

[Samenvatting 2](#_Toc120532752)

[Inleiding 5](#_Toc120532753)

[Over dit rapport 5](#_Toc120532754)

[Data Protection Impact Assessment 5](#_Toc120532755)

[Scope 6](#_Toc120532756)

[Methodologie 6](#_Toc120532757)

[Opzet van de DPIA 6](#_Toc120532758)

[DEEL A 8](#_Toc120532759)

[1. Voorstel 9](#_Toc120532760)

[2. Persoonsgegevens 10](#_Toc120532761)

[3. Gegevensverwerkingen 12](#_Toc120532762)

[4. Verwerkingsdoeleinden 14](#_Toc120532763)

[5. Betrokken partijen 15](#_Toc120532764)

[6. Belangen bij de gegevensverwerkingen 16](#_Toc120532765)

[6.1. Belangen [partij 1 - verantwoordelijke] 16](#_Toc120532766)

[6.2. Belangen [partij 2 – verwerker/leverancier] 16](#_Toc120532767)

[6.3. Belangen partij 3 – betrokkene 16](#_Toc120532768)

[6.4. Belangen [partij 4 - ] 16](#_Toc120532769)

[7. Verwerkingslocaties 17](#_Toc120532770)

[8. Technieken en methoden van de gegevensverwerkingen 18](#_Toc120532771)

[9. Juridisch en beleidsmatig kader 19](#_Toc120532772)

[9.1. Algemene wet- en regelgeving 19](#_Toc120532773)

[9.2. Specifieke wet- en regelgeving 19](#_Toc120532774)

[9.3. Beleidsmatig kader 19](#_Toc120532775)

[10. Bewaartermijnen 20](#_Toc120532776)

[DEEL B 21](#_Toc120532777)

[11. Rechtsgrond 22](#_Toc120532778)

[12. Bijzondere persoonsgegevens 23](#_Toc120532779)

[13. Doelbinding 24](#_Toc120532780)

[14. Noodzaak en evenredigheid 25](#_Toc120532781)

[14.1. Beoordeling proportionaliteit 25](#_Toc120532782)

[14.2. Beoordeling subsidiariteit 26](#_Toc120532783)

[15. Rechten van betrokkenen 27](#_Toc120532784)

[DEEL C 28](#_Toc120532785)

[16. Risico’s 29](#_Toc120532786)

[16.1. Toelichting 29](#_Toc120532787)

[16.2. Mogelijke risico’s 30](#_Toc120532788)

[16.2.1. Risico 1 30](#_Toc120532789)

[16.2.2. Risico 2 30](#_Toc120532790)

[16.2.3. Risico 3 30](#_Toc120532791)

[16.3. Risicomatrix 31](#_Toc120532792)

[DEEL D 32](#_Toc120532793)

[17. Maatregelen 33](#_Toc120532794)

[17.1. Overzicht van maatregelen 33](#_Toc120532795)

[17.2. Beoordeling risico’s na nemen maatregelen 34](#_Toc120532796)

[17.3. Conclusie 34](#_Toc120532797)

[Bijlage 1: 36](#_Toc120532798)

# Inleiding

## Over dit rapport

## Data Protection Impact Assessment

Een Data Protection Impact Assessment (Gegevensbeschermingseffectbeoordeling, hierna: DPIA) is een instrument om bij (voorgenomen) verwerkingen van persoonsgegevens, de risico’s voor betrokkenen op een gestructureerde en gestandaardiseerde wijze in kaart te brengen en te beoordelen. Op basis van de DPIA kan de verantwoordelijke voorafgaand aan de gegevensverwerking maatregelen treffen om negatieve effecten voor betrokkenen te voorkomen of te verkleinen. Een DPIA helpt om te beoordelen of een voorgenomen gegevensverwerking in lijn is met de AVG en andere relevante wetgeving op het gebied van privacy en gegevensbescherming (compliance). Het resulteert niet in een rechtmatigheidsoordeel.

Een DPIA werd vroeger ook aangeduid als PIA, *privacy impact assessment*. Volgens de AVG gaat een DPIA over de risico’s voor de rechten en vrijheden van natuurlijke personen. Betrokkenen hebben een *grondrecht* op bescherming van hun persoonsgegevens en een aantal andere fundamentele *vrijheden* die geraakt kunnen worden door de verwerking van persoonsgegevens. Het recht op gegevensbescherming is dus een breder recht dan alleen het recht op privacy. Overweging 4 van de AVG licht toe: “*Deze verordening eerbiedigt alle grondrechten alsook de vrijheden en beginselen die zijn erkend in het Handvest zoals dat in de Verdragen is verankerd, met name de eerbiediging van het privéleven en het familie- en gezinsleven, woning en communicatie, de bescherming van persoonsgegevens, de vrijheid van gedachte, geweten en godsdienst, de vrijheid van meningsuiting en van informatie, de vrijheid van ondernemerschap, het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht, en het recht op culturele, godsdienstige en taalkundige verscheidenheid*.” In dit rapport wordt niettemin ter wille van de leesbaarheid soms de term ‘privacyrisico’ gebruikt om deze risico’s voor de rechten en vrijheden van betrokkenen aan te duiden, en niet de juridisch correcte term ‘dataprotectierisico’ of ‘gegevensbeschermingsrisico’.

Op grond van artikel 35 van de Algemene Verordening Gegevensbescherming (AVG) is een DPIA in bepaalde gevallen verplicht. Dit is het geval als een voorgenomen gegevensverwerking een hoog risico vormt voor de betrokkenen van wie de persoonsgegevens worden verwerkt. De Autoriteit Persoonsgegevens (AP) heeft een lijst gepubliceerd met 16 soorten verwerkingen waarvoor een DPIA in Nederland altijd verplicht is.3 Wanneer een verwerking niet in deze lijst staat, moet een organisatie zelf beoordelen of het gaat om een gegevensverwerking die waarschijnlijk een hoog risico oplevert. De Europese toezichthouders op de bescherming van persoonsgegevens (de data protection authorities, verenigd in het Europees Comité voor de Gegevensbescherming) hebben negen criteria opgesteld om te beoordelen of het gaat om een dergelijke hoog risico verwerking. De vuistregel is dat een DPIA moet worden uitgevoerd als een verwerking aan twee of meer van de negen criteria voldoet.[[1]](#footnote-1)

[Geef eventueel aan welke indicatoren van toepassing zijn, waardoor de DPIA verplicht is. Check voetnoten].

## Scope

[beschrijf scope, welke proces, verwerking, systeem.

En vooral wat is buiten scope.

## Methodologie

\_\_\_\_\_\_\_ heeft verschillende onderzoeksmethoden toegepast:

## Opzet van de DPIA

\_\_\_\_\_\_\_ heeft deze DPIA uitgevoerd tussen [startmaand] en [eindmaand] [jaartal].

De DPIA volgt de structuur van het *Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA)*.8 Dit model bestaat uit de onderstaande vier delen:

1. beschrijving van de kenmerken en doeleinden van de gegevensverwerking
2. beoordeling van de rechtmatigheid van de gegevensverwerking
3. beschrijving en beoordeling van de risico’s voor betrokkenen
4. beschrijving van de voorgenomen maatregelen

Deel A beschrijft de kenmerken en doeleinden van de gegevensverwerking. Ook komen de soorten persoonsgegevens, de betrokkenen, verwerkingsdoeleinden, rollen van de betrokken partijen, belangen bij de verwerking, locaties waar de gegevens worden verwerkt en bewaartermijnen aan de orde. De (technische) werking van de xxx software/proces/verwerking/systeem komt in dit deel ook aan bod.

Deel B beoordeelt de grondslagen, de noodzaak, evenredigheid en verenigbaarheid van de voorgenomen verwerkingen in relatie tot de verwerkingsdoeleinden. De evenredigheid wordt beoordeeld in het licht van de principes van gegevensverwerking zoals opgesomd in artikel 5 van de AVG, zoals transparantie, adequate beveiliging, *privacy by design* en doelbinding. In dit deel wordt ook de rechtmatigheid beoordeeld van doorgifte van persoonsgegevens naar landen buiten de EU, en de wijze waarop de rechten van betrokkenen worden gewaarborgd.

Deel C beschrijft en beoordeelt de risico’s voor de rechten en vrijheden van betrokkenen die voortvloeien uit de verwerking van persoonsgegevens in de software/proces/verwerking/systeem. Aanvullend is hier een overzicht opgenomen van mogelijke risico’s bij breder gebruik van Microsoft toepassingen.

Deel D beschrijft de aanvullende technische en organisatorische maatregelen die nodig zijn om de geconstateerde resterende privacyrisico’s te verlagen of weg te nemen. Tot slot beschrijft dit deel of er sprake is van een restrisico van de gegevensverwerking na toepassing van risico verlagende maatregelen.

# DEEL A

# Voorstel

Beschrijf het voorstel waar de gegevensbeschermingseffectbeoordeling op ziet en de context waarbinnen deze plaatsvindt op hoofdlijnen.

# Persoonsgegevens

Het begrip persoonsgegevens is breed en behelst allerlei soorten gegevens over een persoon.

"persoonsgegevens": alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

In de tabel hieronder staan de persoonsgegevens die in het kader van deze DPIA relevant zijn.

|  |  |  |
| --- | --- | --- |
| **Bericht** | **Gegevens (data)** | **Persoonsgegevens**  |
| **Lusdetectiedata** |  |  |
| **Streaming – Vlog** |  |  |
| **SRM** |  |  |
| **CAM** |  |  |
| **SSM** |  |  |
| **SPaT** |  |  |
| **MAP** |  |  |
| **DENM** |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type persoonsgegevens | Ja/nee | Verkregen van | Categorie persoonsgegevens | Categorie betrokkenen |
| Persoonsgegevens in het algemeen  |  | BetrokkeneAnders |  | Weggebruiker  |
| Bijzondere persoonsgegevens | **Nee** |  |  |  |

# Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer.

Het verwerken van gegevens is een breed begrip:

"verwerking": een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals 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 gegevens;

Het verwerken omvat de hele levenscyclus van persoonsgegevens.



# Verwerkingsdoeleinden

Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

Lijst doeleinden invoegen

Maak hierbij onderscheid tussen de doeleinden van verschillende partijen. Als er een verwerker is die op basis van algemene voorwaarden of anderszins ook eigen doeleinden bepaalt, dan moeten die hier worden opgenomen.

[opvragen bij opdrachtgever]

# Betrokken partijen

Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker en ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

Analyseer op basis van contracten en voorwaarden of een verwerker daadwerkelijk alleen verwerker is. Als er ook eigen doeleinden worden bepaald zal de verwerker ook (deels) (gezamenlijk) verwerkingsverantwoordelijke zijn.

[kijk naar contracten en feitelijke situatie]

[controleer of er nog derde partijen zijn die buiten beeld toch gegevens verkrijgen]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Partij | Rol  | Functies met toegang  |  |  |
| 1 | Verwerkingsverantwoordelijke (evt. gezamenlijk), verwerker, verstrekker of ontvanger | Functionarissen met toegang |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |

Tabel opmaken

# Belangen bij de gegevensverwerkingen

Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenomen gegevensverwerkingen.

Lijstje belangen

* Financiële / commerciële belangen
* Voldoen aan wettelijke plicht
* Efficiëntie en bedrijfsvoering
* Uitvoering geven aan publieke taak
* Klantrelaties / marketing
* Leveren goede dienst
* Beveiliging van de gegevens
* Fraudebestrijding
* [aanvullen]

## Belangen [partij 1 - verantwoordelijke]

## Belangen [partij 2 – verwerker/leverancier]

## Belangen partij 3 – betrokkene

## Belangen [partij 4 - ]

# Verwerkingslocaties

Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

Europese Unie / Europese Economische Ruimte

* Ierland
* Nederland

Let op bij Verenigd Koninkrijk ivm Brexit. Veel internationale aanbieders van cloudopslag maken al onderscheid tussen Europa en VK.

Let op bij Verenigde Staten: controleer altijd of een partij gevestigd is in de VS of mogelijk toegang heeft tot de data (ook al wordt deze dat niet in de VS opgeslagen). Controleer daarbij de actuele geldigheid van het EU-US Data Privacy Framework (DPF) en of de organisatie gecertificeerd is onder het EU-US DPF (zie: <https://www.dataprivacyframework.gov/list>).

Soms is er per onderdeel van de dienst een verschil in afbakening van de verwerkingslocatie. Denk aan de basisdienst en contentopslag binnen EU, maar technische support mogelijk overal ter wereld. Splits dat dan uit.

Tabel met land en eventueel specifieke locatie. En eventueel nog invoegen eigen hosting of externe partij.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Land | EER | Beheer hosting |  |
|  |  | Ja/Nee |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Eventueel visual toevoegen met landkaart (bijvoorbeeld via excel te maken)

# Technieken en methoden van de gegevensverwerkingen

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

|  |  |  |  |
| --- | --- | --- | --- |
| Verwerking | Geautomatiseerde besluitvorming | Profilering  | Big data verwerkingen |
|  | Ja/nee | Ja/nee | Ja/nee |
|  |  |  |  |

# Juridisch en beleidsmatig kader

Noem ook sectorspecifieke wet- en regelgeving.

De volgende wet- en regelgeving is van toepassing op de verwerking.

## Algemene wet- en regelgeving

|  |  |  |  |
| --- | --- | --- | --- |
|  | Wet- en regeleging |  | Artikel (optioneel) |
|  | Algemene Verordening Gegevensbescherming | √ |  |
|  | Uitvoeringswet Algemene Verordening Gegevensbescherming |  |  |
|  | Gedragscodes | - | 40 AVG |
|  | Certificering | - | 42 AVG |
|  | Adequaatheidsbesluit | - | 45 AVG |
|  | Standaard contractsbepalingen | - | 46 AVG |
|  | Bindende bedrijfsvoorschriften | - | 47 AVG |
|  | … |  |  |

## Specifieke wet- en regelgeving

|  |  |  |  |
| --- | --- | --- | --- |
|  | Wet- en regelgeving |  | Artikel (optioneel) |
|  | Wegenverkeerswet  |  |  |
|  | Burgerlijk Wetboek |  | Art. 6:174 van het Burgerlijk Wetboek |
|  | … |  |  |

## Beleidsmatig kader

|  |  |  |  |
| --- | --- | --- | --- |
|  | Beleidsmatig kader |  | Artikel (optioneel) |
|  | Interne beleidsdocumenten |  |  |
|  | Contracten met andere partijen |  |  |
|  | … |  |  |

# Bewaartermijnen

Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Categorie persoonsgegevens | Ingang bewaartermijn | Termijn van bewaring | Motivatie bewaring | Verantwoordelijkheid voor verwijdering |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# DEEL B

# Rechtsgrond

Bespreek alle rechtsgronden die in het kader van de DPIA relevant kunnen zijn.

Bij overheidsorganisaties: grondslag e voor publieke taak, maar in bedrijfsvoering grondslag f. Er is discussie aan het komen of het niet altijd alleen e kan zijn, dus daarom mogelijk e en f samen behandelen. De afweging blijft hetzelfde en moet onderbouwd worden. En ook de noodzakelijkheid.

* Rechtsgronden weergeven (a tm f).
* Noodzakelijk voor de uitvoering van een overeenkomst
* Naleven wettelijke verplichting

Zes rechtsgronden beschrijven. In deze DPIA zijn de volgende relevant.

# Bijzondere persoonsgegevens

Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dit is toegestaan.

Zie tabel bij hoofdstuk 2.

Op grond van artikel 9 van de AVG is de verwerking van bijzondere persoonsgegevens verboden, tenzij een van de wettelijke uitzonderingen van toepassing is.

# Doelbinding

Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.

Verenigbaarheidstoets (legitimate interest assessment of LIA) – check of er lijstjes zijn.

Zie ook hoofdstuk 4.

Doelbinding is één van de kernbeginselen uit artikel 5 van de AVG. In artikel 5(1)b is gespecificeerd dat persoonsgegevens alleen voor **welbepaalde**, **uitdrukkelijk omschreven** en **gerechtvaardigde doeleinden** mogen worden verzameld en vervolgens niet verder mogen verwerkt op een met die doeleinden onverenigbare wijze worden verwerkt. Verantwoordelijken moeten kunnen bewijzen op grond van artikel 5(2) van de AVG dat zij dit beginsel naleven (verantwoordingsplicht).

# Noodzaak en evenredigheid

Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit.

a. Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden

b. Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder

Alle gegevensverwerkingen moeten voldoen aan de beginselen van noodzaak en evenredigheid. Het begrip noodzaak bestaat uit twee samenhangende begrippen, namelijk proportionaliteit en subsidiariteit. De persoonsgegevens die worden verwerkt, moeten noodzakelijk zijn voor het doel van de verwerking. **Proportionaliteit** betekent dat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding staat tot de verwerkingsdoeleinden. **Subsidiariteit** betekent dat de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, kunnen worden verwezenlijkt.

Evenredigheid betekent dat er een evenwicht is tussen de belangen van de betrokkene en de belangen van de verwerkingsverantwoordelijke. Een evenredige gegevensverwerking houdt in dat de hoeveelheid verwerkte gegevens niet buitensporig is in verhouding tot het doel van de verwerking. Als een verantwoordelijke zijn doel kan bereiken door minder persoonsgegevens te verwerken, moet hij de hoeveelheid verwerkte persoonsgegevens beperken tot wat noodzakelijk is.

Daarom mag een verantwoordelijke alleen die persoonsgegevens verwerken die noodzakelijk zijn om het legitieme doel te bereiken, maar geen persoonsgegevens waar hij ook buiten kan. De toepassing van het beginsel van proportionaliteit is dus nauw verwant aan de beginselen van dataprotectie uit artikel 5 van de AVG.

## Beoordeling proportionaliteit

De kernvragen zijn: zijn de belangen goed afgewogen? En gaat de verwerking niet verder dan wat nodig is? Om te beoordelen of de verwerking in verhouding staat tot het belang van de verwerkingsverantwoordelijke(n), moet de verwerking voldoen aan de beginselen van artikel 5 van de AVG.

De gegevens moeten “**rechtmatig, eerlijk en transparant** worden verwerkt ten opzichte van de betrokkenen” (artikel 5, lid 1, onder a), van de AVG). Dit betekent dat de betrokkenen op de hoogte moeten worden gebracht van de verwerking van hun gegevens, dat alle wettelijke voorwaarden voor gegevensverwerking worden nageleefd en dat het evenredigheidsbeginsel in acht wordt genomen.

Aanvullen met specifieke info DPIA

## Beoordeling subsidiariteit

De hamvraag bij dit onderdeel van de beoordeling van de noodzaak van de verwerkingen is of dezelfde doelen bereikt kunnen worden met minder inbreukmakende middelen.

# Rechten van betrokkenen

Geef aan hoe invulling wordt gegeven aan de rechten van de betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzondering dat is toegestaan.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | Geregeld? | Korte beschrijving hoe? |
|  | Recht op informatie  | Ja/nee |  |
|  | Recht op inzage  |  |  |
|  | Recht op correctie  |  |  |
|  | Recht op verwijdering  |  |  |
|  | Recht op beperking van de verwerking  |  |  |
|  | Recht van bezwaar  |  |  |
|  | Recht van herroeping  |  |  |

# DEEL C

# Risico’s

## Toelichting

Een DPIA gaat over de risico’s voor betrokkenen. Dus niet zozeer over de beveiligings-, continuïteits- of andere risico’s die de organisatie die de DPIA uitvoert loopt. Dit maakt de insteek verwant aan die van andere vakgebieden, maar is deze toch fundamenteel anders dan de risico analyses uit die andere vakgebieden.

In dit hoofdstuk worden de risico’s bepaald en onderzocht wat de kans en gevolgen van de risico’s zijn. In Deel D volgen de maatregelen waarmee de risico’s eventueel beperkt (gemitigeerd) kunnen worden.

De Engelse toezichthouder ICO heeft een lijst met hoofdcategorieën van risico’s opgesteld.

* Verlies van controle op het gebruik van de gegevens
* Verlies van vertrouwelijkheid
* Onmogelijkheid voor betrokkenen om hun rechten uit te oefenen
* Heridentificatie van gepseudonimiseerde gegevens
* Onrechtmatige (verdere) verwerking

Op basis van deze algemene lijst met risico kunnen de specifieke risico’s binnen deze DPIA worden vastgesteld en vervolgens worden geplot in een zogenaamde risicomatrix. Zie daarvoor het figuur hieronder. De uitkomst (het risico) wordt bepaald aan de hand van de gevolgen (minimaal, enige, ernstige) en de kans (heel klein, redelijke mogelijkheid, waarschijnlijker dan niet). De invulling van de kans en de gevolgen vraagt een inschatting.

ImpactHoog –De gevolgen voor de betrokkene hebben bij het materialen van het risico forse invloed op het leven van de betrokkeneMiddel –De gevolgen voor de betrokkene hebben bij materialiseren van het risico geen beperkteimpact op het leven van de betrokkeneLaag –De gevolgen voor de betrokkene hebben materialiseren van het risico weinig of verwaarloosbare invloed op het leven van de betrokkene

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ernst van de gevolgen voor de betrokkene(n)** | Ernstige gevolgen | Laag risico  | Hoog risico  | Hoog risico  |
| Enige negatieve gevolgen | Laag risico | Medium risico | Hoog risico  |
| Minimale gevolgen | Laag risico | Laag risico | Laag risico   |
|   | Heel klein  | Redelijke mogelijkheid | Waarschijnlijker dan niet |
|   |   | **Kans (waarschijnlijkheid) dat het risico zich voordoet** |

## Mogelijke risico’s

Bij de uitvoering van deze DPIA zijn de volgende risico’s geïdentificeerd.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Risico | Oorzaak risico | Aard risico | Kans | Impact |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Hieronder volgt een korte toelichting van de risico’s.

### Risico 1

[korte uitwerking]

### Risico 2

[korte uitwerking]

### Risico 3

[korte uitwerking]

Lijst risico’s met subrisicos op basis van presentatie voor gemeente Amsterdam.

## Risicomatrix

Op basis van het voorgaande volgt de risicomatrix

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ernst van de gevolgen voor de betrokkene(n)** | Ernstige gevolgen | Laag risico  | Hoog risico  | Hoog risico  |
| Enige negatieve gevolgen | Laag risico | Medium risico | Hoog risico  |
| Minimale gevolgen | Laag risico | Laag risico | Laag risico   |
|   | Heel klein  | Redelijke mogelijkheid | Waarschijnlijker dan niet |
|   |   | **Kans (waarschijnlijkheid) dat het risico zich voordoet** |

# DEEL D

# Maatregelen

* Maatregelen koppelen aan de genoemde risico’s. Dat kan met de nummers als referentie.
* Maak voor de maatregelen onderscheid tussen welke betrokken partijen de maatregelen moeten treffen.
* Beoordeel of na het treffen van de maatregelen er geen hoge risico’s meer resteren.

## Overzicht van maatregelen

|  |  |  |  |
| --- | --- | --- | --- |
| Nr. | Risico | Soort Maatregelen | Aanbevolen maatregel |
|  |  | Technisch/organisatorisch |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk no.** | **Omschrijving risico** | **Risico beoordeling** | **Maatregelen** |
| 1 | Inability to effectively withdraw consent, may include special categories of data. | Laag / medium/ hoog | Setup procedures to process the withdrawing of consent, in particular for special categories of personal data. |
| 2 | Lack of control over processing of special categories of data |  | Exclude special categories and other sensitive data from storage in audit tables, or: |
|  | Stop using the audit tables. |
| 3 | Incomplete implementation of legitimate interest |  | Formulate and assess the legitimate interest of the Council of State for the indicated processings, and balance this legitimate interest with the interests, rights and freedoms of the data subjects. |
| 5 | Inability to delete personal data of contact persons the CRM system after expiration of retention period |  | Limit the retention of data in audit tables to what is necessary for the purposes for which the data is collected, and implement controls to respect those retention limits. |
| 6 | Inability to exercise data subject rights |  | Perform a specific audit on whether Microsoft acts according to the agreed contractual measures in Azure AD. |

## Beoordeling risico’s na nemen maatregelen

Als er nog het nemen van de maatregelen nog hoge risico’s overblijven, dan is consultatie bij Autoriteit Persoonsgegevens nodig.

Op basis van bovenstaande analyse volgt dat na het nemen van de maatregelen

## Conclusie

Korte samenvatting uitkomsten.

Indien alle maatregelen worden getroffen, dan is uiteindelijk de uitkomst…

De uiteindelijke aanbeveling is om de software/proces/dienst/systeem [kies een optie]

1. uit te rollen
2. aan te passen op de volgende wijze
3. af te blazen



Voor vragen, neem contact op met [contactpersoon].

[www.privacycompany.eu](http://www.privacycompany.eu)
info@privacycompany.nl
070 – 820 96 90

Maanweg 174
2516 AB Den Haag
14e verdieping

Postbus 95315
2509 CH Den Haag

Bijlage 1:

1. [↑](#footnote-ref-1)