|  |  |  |
| --- | --- | --- |
|  |  |  |
| DPIA <naam proces> |  |  |
| <naam opdrachtgever> |  |  |
|  |  |  |
| Sparrenheuvel 32, 3708 JE Zeist | (030) 2 270 500 | [info@mxi.nl](mailto:offertebureau@mxi.nl) | [www.mxi.nl](http://www.mxi.nl) | |  | Project |
|  |  | Datum |
|  |  |  |

Inhoudsopgave

[1 managementsamenvatting 4](#_Toc165363492)

[2 Inleiding 6](#_Toc165363493)

[2.1 Uitvoering van de DPIA 6](#_Toc165363494)

[2.2 Definities 6](#_Toc165363495)

[2.3 Achtergrondinformatie 7](#_Toc165363496)

[FASE](#_Toc165363500) 0

[3 PreDPIA 11](#_Toc165363501)

[3.1 De verwerking 11](#_Toc165363502)

[3.2 Waarom een DPIA? 11](#_Toc165363504)

[FASE](#_Toc165363505) 1

[4 beschrijving 13](#_Toc165363506)

[4.1 Scope van de DPIA 13](#_Toc165363507)

[4.2 Doel van de gegevensverwerking 13](#_Toc165363508)

[4.3 Categorieën persoonsgegevens 13](#_Toc165363509)

[4.4 Uitvoering 13](#_Toc165363510)

[4.5 Betrokken applicaties en partijen bij de verwerking 13](#_Toc165363511)

[4.6 Systematische beschrijving 14](#_Toc165363512)

[5 beoordeling 15](#_Toc165363513)

[5.1 Rechtsgrond voor de verwerking van persoonsgegevens 15](#_Toc165363514)

[5.2 Dataminimalisatie en bewaartermijnen 16](#_Toc165363517)

[5.3 Waarborgen voor de rechten van betrokkenen 17](#_Toc165363520)

[6 risico’s en maatregelen 19](#_Toc165363523)

[6.1 Risico-inventarisatie 19](#_Toc165363524)

[7 Advies functionaris gegevensbescherming 21](#_Toc165363527)

[8 inbreng betrokkenen 22](#_Toc165363528)

[9 procesverantwoordelijke 23](#_Toc165363529)

[FASE](#_Toc165363530) 2

[10 implementie van maatregelen 25](#_Toc165363531)

[BIJLAGE 1: Geraadpleegde bronnen 26](#_Toc165363535)

|  |
| --- |
| 1.Inleiding.jpg  Info inleiding.png |

# managementsamenvatting

Deze DPIA is uitgevoerd op het <proces>, die de <verwerkingsverantwoordelijke> als verwerkingsverantwoordelijke uitvoert.

**Rechtmatigheid**

De grondslag voor deze verwerking is bepaald als: <grondslag>.

De uitwerking van deze grondslag en nadere toelichting zijn te vinden in hoofdstuk 6 van dit rapport.

**Risico’s**

We voorzien binnen deze verwerking een aantal hoge risico’s waarvoor wij maatregelen adviseren. Deze staan beschreven in de tabel hieronder.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| # | Omschrijving | K | I | R | Beoogde maatregel | K | I | RR |
|  |  |  |  |  |  |  |  |  |

**Legenda**

K = Kans

I = Impact

R = Risico (= K\*I)

RR = Rest-risico (= K\*I)

Een volledig overzicht van de risico’s is opgenomen in hoofdstuk 6.

**Belangrijkste maatregelen**

Op basis van de bevindingen van deze DPIA zijn een aantal algemene maatregelen geformuleerd, waarmee de belangrijkste en/of meerdere risico’s gemitigeerd kunnen worden:

* Maatregel 1
* Maatregel 2
* Maatregel 3

# Inleiding

## uitvoering van de DPIA

Gedurende de uitvoering van de DPIA zijn de volgende personen betrokken:

|  |  |  |  |
| --- | --- | --- | --- |
| **Fase** | **Onderdeel** | **Functie** | **Naam** |
| 0 | PreDPIA |  |  |
| 1 | Beschrijving |  |  |
|  | Beoordeling |  |  |
|  | Risicoworkshop |  |  |
|  | Validatiesessie |  |  |
|  | Beoordeling DPIA | Functionaris Gegevensbescherming |  |
| 2 | Vaststellen van de maatregelen | Proceseigenaar |  |

**Datum en geldigheid**

Deze DPIA is afgerond op <datum>. De DPIA zal herzien worden in <kwartaal en jaartal>.

## definities

<Verwerkingsverantwoordelijke>

Organisatie en alle dochterorganisaties.

AP

De Autoriteit Persoonsgegevens is de Nederlandse gegevensbeschermingsautoriteit en het zelfstandig bestuursorgaan dat in Nederland bij wet als toezichthouder is aangesteld voor het toezicht op het verwerken van persoonsgegevens.

AVG

Algemene Verordening Gegevensbescherming

DPIA

Een data protection impact assessment (gegevensbeschermingeffectbeoordeling) is een proces waarin een verwerking systematisch beschreven en geanalyseerd wordt. Voor afronding van een DPIA is naast beschrijving van de verwerking een analyse noodzakelijk van alle risico’s, inclusief de bijbehorende maatregelen. Pas wanneer deze maatregelen geaccepteerd zijn (en dus toegezegd is dat deze gestart gaan worden) kan de DPIA formeel worden afgerond.

**FG**

De Functionaris Gegevensbescherming, die toezicht houdt op de uitvoering van de AVG binnen een specifieke organisatie waar hij/zij is aangesteld.

## Achtergrondinformatie

Dit rapport bevat de vastlegging van de uitgevoerde , data protection impact assessment (DPIA) die uitgevoerd is op het <proces>.

### Wat is een DPIA?

Een DPIA, data protection impact assessment (Nederlands: gegevensbeschermingeffectbeoordeling), is volgens de definitie van de AP:

*“.. een instrument om vooraf de privacyrisico’s van een gegevensverwerking in kaart te brengen. Zodat de organisatie maatregelen te kunnen nemen om de risico’s te verkleinen.”[[1]](#footnote-2)*

Door tijdig en adequaat DPIA’s uit te voeren krijg je als organisatie grip op de risico’s die je loopt op het gebied van privacy. De verbeterde grip op privacybescherming vertaalt zich in de regel ook vaak door verbeteringen in informatiebeveiliging, omdat hier de beoogde/gewenste maatregelen zitten.

Doel DPIA

De DPIA is een proces dat is bedoeld om de verwerking van persoonsgegevens te beschrijven, de noodzaak en evenredigheid ervan te beoordelen en de aan de verwerking verbonden risico’s voor de rechten van vrijheden en van natuurlijke personen te identificeren door deze risico’s in te schatten en de maatregelen ter beperking van die risico’s te beoordelen. De DPIA, overeenkomstig de AVG, is een instrument om risico's voor de rechten van de betrokkenen te beheersen, waarbij dus hun perspectief wordt ingenomen.

### Uitvoering van een DPIA

Voor het uitvoeren van de DPIA zoals deze in dit document is beschreven, is gebruik gemaakt van het DPIA stappenplan van M&I/Partners. De rest van dit rapport volgt de structuur van dit stappenplan.   
  
Dit stappenplan ziet er als volgt uit:

Afbeelding met tekst, schermopname, Website, Webpagina

Automatisch gegenereerde beschrijving

<Fase 2 valt buiten scope van de opdracht en is derhalve niet in dit rapport opgenomen>

### Leeswijzer en geldigheid

Deze DPIA is als volgt opgebouwd:

* Fase 0
  + Hoofdstuk 3 bevat de PreDPIA, met een compacte beschrijving van de verwerking, waarbij wordt toegelicht waarom een DPIA nodig is.
* Fase 1
  + In hoofdstuk 4 volgt een uitgebreide beschrijving van de verwerking, bestaande uit;
    - de scope.
    - de doelen van de processen binnen de verwerking.
    - de categorieën ontvangers.
    - de betrokken partijen.
    - een concrete, systematische beschrijving van alle processen binnen de verwerking.
  + De beoordeling in hoofdstuk 5 toetst de verwerking binnen de gestelde kaders van de AVG;
  + Hoofdstuk 6 bevat een risicoanalyse van de vastgestelde risico’s en maatregelen;
  + In hoofdstuk 7 geeft de FG een reactie op de uitvoering van de DPIA, de rapportage en de geadviseerde maatregelen.
  + In hoofdstuk 8 is ruimte voor een reactie van betrokkenen.
  + Hoofdstuk 9 bevat het akkoord van de procesverantwoordelijke.
* Fase 2
  + In hoofdstuk 10 wordt een plan van aanpak toegevoegd over de vastgestelde maatregelen.
* Bijlage
  + Bijlage 1 bevat een overzicht van de geraadpleegde bronnen.

**Belangrijk:** Deze DPIA is van toepassing op de scope en processen zoals beschreven in hoofdstuk 4. Bij wijzigingen in van processen en/of van de vastgelegde persoonsgegevens zal getoetst moeten worden of de uitgevoerde DPIA nog geldig is of dat er een nieuwe toets moet plaatsvinden.

Fase 0

**FASE 0**

# PreDPIA

## DE VERWERKING

De verwerking <naam verwerking> heeft als doel <beschrijving van het doel en de organisatie waarbinnen de verwerking zich afspeelt>.

### Korte beschrijving van het proces

<Voeg een korte beschrijving toe van het proces, zodat ook buitenstaanders begrijpen hoe dit proces loopt>

## WAAROM EEN DPIA?

Er is besloten om een DPIA te doen op deze verwerking, omdat er sprake is van een (mogelijk) hoog risico op de rechten en vrijheden van betrokkenen.

<Voeg hier de PreDPIA toe, inclusief de beoordeling door de FG/Privacy jurist/privacy officer.”.>

Tussenblad: fase 1

**FASE 1**

# beschrijving

## SCOPE VAN DE DPIA

De scope van de DPIA is met zwarte omlijning aangegeven op onderstaande procesplaat. De diverse processen binnen deze DPIA staan beschreven in paragraaf 5.7.

<Procesplaat invoegen, indien nodig toelichting geven op de scope>

## DOEL VAN DE GEGEVENSVERWERKING

Het doel van de gegevensverwerking is: <doel van de gegevensverwerking>

Subdoelen zijn:

* <Subdoel 1;
* Subdoel 2;
* Subdoel 3>.

## CATEGORIEËN PERSOONSGEGEVENS

De volgende categorieën persoonsgegevens worden verwerkt:

* Standaard persoonsgegevens:
  + <Categorische opsomming van de persoonsgegevens die worden verwerkt.>.
  + <Categorische opsomming van de persoonsgegevens die worden verwerkt.>.
  + <Categorische opsomming van de persoonsgegevens die worden verwerkt.>.
  + <Categorische opsomming van de persoonsgegevens die worden verwerkt.>.
  + <Categorische opsomming van de persoonsgegevens die worden verwerkt.>.
* Bijzondere persoonsgegevens:
  + <Categorische opsomming van de persoonsgegevens die worden verwerkt.>.
  + <Categorische opsomming van de persoonsgegevens die worden verwerkt.>.

## UITVOERING

<Maak een tekstuele beschrijving van de verwerking. Beschrijven op welke wijze de uitvoering van de verschillende stappen in de verwerking plaatsvindt (handmatig, automatisch, profiling)>

## BETROKKEN APPLICATIES EN PARTIJEN BIJ DE VERWERKING

Bij de verwerking zijn de volgende partijen betrokken:

|  |  |  |
| --- | --- | --- |
| **Naam partij** | **Rol van partij bij de verwerking** | **Document waar afspraken zijn vastgelegd (indien van toepassing)** |
|  |  |  |

De verwerking vindt plaats in de volgende applicaties:

|  |  |  |  |
| --- | --- | --- | --- |
| **Naam applicatie** | **Leverancier** | **Interne eigenaar** | **Verwerkersovereenkomst aanwezig?** |
|  |  |  |  |

<Voeg hier een toelichting toe waarin beschreven wordt welke partijen verwerkingsverantwoordelijke, verwerker en eventueel subverwerker zijn en welke taken zij uitvoeren. Hou ook rekening met de mogelijkheid dat partijen gezamenlijk verwerkingsverantwoordelijke zijn>

De volgende rollen/functies zijn betrokken bij de verwerking:

|  |  |  |  |
| --- | --- | --- | --- |
| **Organisatie** | **Rol/functie** | **Bevoegdheden/takenpakket** | |
|  |  |  |
|  |  |  |
|  |  |  |

## SYSTEMATISCHE BESCHRIJVING

Voor de systematische beschrijving van <naam verwerking>, is een gegevensstroomanalyse opgesteld.  
Er is splitsing gemaakt in de volgende subverwerkingen:

<Verwerking 1>

* + <Subverwerking a>.

<Verwerking 2>

* + <Subverwerking b>.

Het doel van deze gegevensstroomanalyse is het in kaart brengen van de levenscyclus van de persoonsgegevens. We beschrijven in iedere gegevensstroomanalyse deze cyclus aan de hand van de laagdrempelige [bronnen + input – verwerking – output + ontvangers]-structuur.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. Naam proces | | | | |
| Bron | Input | Verwerking | Output | Eindbestemming |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| 1a. Naam subverwerking | | | | |
|  |  |  |  |  |
|  |  |  |  |  |
| 1b. Naam subverwerking | | | | |
|  |  |  |  |  |
|  |  |  |  |  |

# beoordeling

## RECHTSGROND voor de verwerking van persoonsgegevens

### Rechtsgrond voor de verwerking van alle persoonsgegevens

De verwerking van gegevens van <betrokkenen> binnen de <Organisatie X> ten behoeve van <proces> is gebaseerd op de volgende grondslag:

* Artikel 6 lid 1 sub a: “de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden”. <Toelichting grondslag, inclusief of er rekening is gehouden met de eisen die aan toestemming gesteld worden, mogelijke machtsverhoudingen en consequenties van het intrekken van toestemming>;
* Artikel 6 lid 1 sub b: “de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen”. <Toelichting grondslag, inclusief welke overeenkomst dit betreft>;
* Artikel 6 lid 1 sub c: “de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust”. <Toelichting grondslag, inclusief welke wet, artikel, lid>;
* Artikel 6 lid 1 sub d: “de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen”. <Toelichting grondslag>;
* Artikel 6 lid 1 sub e: “de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen”. <Toelichting grondslag, inclusief welke wet, artikel, lid>;
* Artikel 6 lid 1 sub f: “verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde”. <Toelichting grondslag, met name waarom de grondrechten en fundamentele vrijheden van de betrokkene niet zwaarder wegen dan het gerechtvaardigde belang van de organisatie>.

### Rechtsgrond voor de verwerking van bijzondere persoonsgegevens

De verwerking van bijzondere persoonsgegevens van <betrokkenen> binnen de <Organisatie X> ten behoeve van <proces> is gebaseerd op de volgende grondslag:

* Artikel 9 lid 2 sub a: “de betrokkene heeft uitdrukkelijke toestemming gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinde.” <Toelichting grondslag, inclusief of er rekening is gehouden met de eisen die aan toestemming gesteld worden, mogelijke machtsverhoudingen en consequenties van het intrekken van toestemming >;
* Artikel 9 lid 2 sub b: “e verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten van de verwerkingsverantwoordelijke of de betrokkene op het gebied van het arbeidsrecht en het socialezekerheids- en socialebeschermingsrecht.” <Toelichting grondslag>
* Artikel 9 lid 2 sub c: “de verwerking is noodzakelijk ter bescherming van de vitale belangen van de betrokkene of van een andere natuurlijke persoon indien de betrokkene fysiek of juridisch niet in staat is zijn toestemming te geven.” <Toelichting grondslag>
* Artikel 9 lid 2 sub d: “de verwerking wordt verricht door een stichting, een vereniging of een andere instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is, in het kader van haar gerechtvaardigde activiteiten en met passende waarborgen, mits de verwerking uitsluitend betrekking heeft op de leden of de voormalige leden van de instantie of op personen die in verband met haar doeleinden regelmatig contact met haar onderhouden, en de persoonsgegevens niet zonder de toestemming van de betrokkenen buiten die instantie worden verstrekt;.” <Toelichting grondslag>
* Artikel 9 lid 2 sub e: “de verwerking heeft betrekking op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;.” <Toelichting grondslag>
* Artikel 9 lid 2 sub f: “de verwerking is noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering of wanneer gerechten handelen in het kader van hun rechtsbevoegdheid;.” <Toelichting grondslag>
* Artikel 9 lid 2 sub g: “de verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht.” <Toelichting grondslag, met name waarom de grondrechten en fundamentele vrijheden van de betrokkene niet zwaarder wegen dan het gerechtvaardigde belang van de organisatie>
* Artikel 9 lid 2 sub h: “de verwerking is noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten, op grond van Unierecht of lidstatelijk recht, of uit hoofde van een overeenkomst met een gezondheidswerker en behoudens de in lid 3 genoemde voorwaarden en waarborgen.” <Toelichting grondslag>
* Artikel 9 lid 2 sub i: “de verwerking is noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid.” <Toelichting grondslag>
* Artikel 9 lid 2 sub j: “de verwerking is noodzakelijk met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig [artikel 89](https://www.privacy-regulation.eu/nl/artikel-89-waarborgen-en-afwijkingen-verband-met-verwerking-met-het-oog-op-archivering-het-algemeen-belang-wetenschappel-EU-AVG.htm) lid 1.” <Toelichting grondslag, inclusief toelichting hoe dit overeenkomstig artikel 89 lid 1 AVG en artikel 24 UAVG is ingericht.>

## DATAMINIMALISATIE EN BEWAARTERMIJNEN

### Dataminimalisatie

Om de privacy van betrokkenen zo goed mogelijk te beschermen, is het belangrijk dat binnen de verwerking <proces> de data zoveel mogelijk geminimaliseerd wordt. Om dit te toetsen, is dataminimalisatie opgesplitst in drie basisprincipes:

* Noodzakelijkheid: zijn deze persoonsgegevens werkelijk nodig voor het doel van de verwerking;
* Proportionaliteit: staat het doel van de verwerking in verhouding tot de inbreuk op privacy van de betrokkene;
* Subsidiariteit: is het niet mogelijk om de verwerking op een minder ingrijpende manier of met minder ingrijpende middelen te bereiken.

Hieronder worden deze drie basisprincipes getoetst.

**Noodzakelijkheid**

<Beschrijf:

* Waarom de organisatie gegevens verwerkt (doelen) en toets in hoeverre de gegevens daadwerkelijk nodig zijn voor het verwerkelijken van het doel;
* Toets of persoonsgegevens worden verwerkt voor andere doelen en in hoeverre deze verenigbaar zijn (artikel 6 lid 4 AVG en artikel 89 AVG);
* Benoem eventuele risico’s en neem deze op in de tabel in hoofdstuk 7.>.

Bij het bepalen van het noodzakelijkheidsprincipe is het daarnaast van belang om in kaart te brengen welke partijen er toegang hebben tot persoonsgegevens van de burger. In dit proces hebben de volgende partijen toegang:

* <Partij 1>.
* <Partij 2>.

<Beschrijf waarom de organisatie gegevens verwerkt (doelen) en toets in hoeverre de personen die toegang hebben tot de gegevens, dit ook werkelijk nodig hebben voor de uitvoer van hun taken.

**Proportionaliteit**

<Beschrijf de inbreuk op de rechten van betrokkenen en beschrijf de doelen van de verwerking. Toets of de inbreuk niet onevenredig is in verhouding tot de doelen.>

**Subsidiariteit**

<Beschrijf:

* of er een minder ingrijpende manier mogelijk is om de doelen van deze gegevensverwerking te bereiken, bijvoorbeeld door het wel/niet inzetten van een applicatie of ketenpartner. Benoem eventuele risico’s en neem deze op in de tabel in hoofdstuk 7.
* De voordelen van de huidige werkwijze t.o.v. andere werkwijzen (bijvoorbeeld gebruik van een beveiligde applicatie ten opzichte van een harde schijf of papier)>

### Bewaartermijnen

**Optie 1:** Voor de persoonsgegevens binnen deze gegevensverwerking zijn de volgende wettelijke bewaartermijnen gesteld:

* <Opsomming bewaartermijnen + relevante wetgeving of Selectielijst>.

**Optie 2**: Er is geen wettelijke bewaartermijn voor de gegevens die in het kader van deze verwerking worden verwerkt, anders dan dat gegevens niet langer mogen bewaard dan nodig (zogeheten opslagbeperking (artikel 5 lid 1 sub e AVG). <Voeg toe welke bewaartermijnen de organisatie gesteld heeft en in hoeverre dit voldoet aan opslagbeperking.>

<Toets in hoeverre er invulling is gegeven aan de opvolging van bewaartermijnen. Benoem eventuele risico’s en neem deze op in de tabel in hoofdstuk 7.>

## WAARBORGEN VOOR RECHTEN VAN BETROKKENEN

### Transparantie

<Betrokkenen> kunnen <via middel, zoals website> een duidelijk overzicht vinden over de verwerkingen die <organisatie x> uitvoert met hun persoonsgegevens. <Benoem eventuele risico’s en neem deze op in de tabel in hoofdstuk 7.>

<organisatie x> verkrijgt:

* <alle gegevens direct van de betrokkene. Als dit het geval is, beschrijf dan ook of de betrokkene voldoende op de hoogte is dat de gegevens die door hem worden aangeleverd, voor deze verwerking worden ingezet>;
* <een deel van de gegevens direct van de betrokkene. Als dit het geval is, beschrijf dan ook of de betrokkene voldoende op de hoogte is dat de gegevens die door hem worden aangeleverd, voor deze verwerking worden ingezet>;
* <geen van de gegevens direct van de betrokkene. Beschrijving ook hier de invloed van de wijze van ontvangen van gegevens op transparantie. Kijk hierbij ook naar het koppelen van gegevens van verschillende bronnen>.

### Uitoefening van rechten

<Beschrijving van hoe rechten van betrokkenen uitgeoefend kunnen worden m.b.t. hier beschreven verwerking. Benoem eventuele risico’s en neem deze op in de tabel in hoofdstuk 6.>

# risico’s en maatregelen

In de onderstaande tabel staat de beoordeling van de risico’s die kunnen leiden tot schending van de privacy van de betrokkene:

* Onrechtmatige toegang tot de persoonsgegevens.
* Ongewenste wijziging van de persoonsgegevens.
* Verdwijning (vernietiging of verlies) van persoonsgegevens.
* Persoonsgegevens zijn (tijdelijk) niet beschikbaar.

Aan de risico’s zijn de beoogde maatregelen toegevoegd om deze risico’s te reduceren.

## RISICO-INVENTARISATIE

In <periode> heeft een werkgroep, bestaande uit <deelnemers aan het DPIA-proces>, een inventarisatie uitgevoerd naar de privacyrisico’s . De risico’s zijn op basis van onderstaande tabel gescoord op kans \* impact = risicoscore.

Impact

|  |  |  |
| --- | --- | --- |
| **Score** | **Impactcategorie** | **Impact** |
| 1 | Geraakte persoonsgegevens | Geen persoonsgegevens betrokken |
|  | Rechten betrokkene | Inbreuk op rechten en vrijheden van 1 betrokkene |
|  | Beveiligingsincident | Geen verlies van gegevens, of verlies van reeds openbare gegevens |
|  | Organisatie | Geringe financiële gevolgen (<€10.000) | Geen imagoschade |
|  | Maatschappij | Geen maatschappelijke gevolgen |
| 2 | Geraakte gegevens | Niet-bijzondere en/of niet-gevoelige gegevens van 1 betrokkene |
|  | Rechten betrokkene | Ernstige tot onherstelbare inbreuk op rechten en vrijheden van 1 betrokkene |
|  | Datalek | Verlies van (niet-bijzondere) persoonsgegevens van een individu |
|  | Organisatie | Matige financiële gevolgen (€10.000 < €100.000) | Lichte imagoschade |
|  | Maatschappij | Lichte maatschappelijke onrust op kleine schaal |
| 3 | Geraakte gegevens | Niet-bijzondere en/of niet-gevoelige gegevens van meerdere betrokkenen of bijzondere of gevoelige gegevens van 1 betrokkene |
|  | Rechten betrokkene | Aanzienlijke inbreuk op rechten en vrijheden van meerdere betrokkenen |
|  | Datalek | Verlies van (niet-bijzondere) persoonsgegevens van meerdere betrokkenen of verlies van gevoelige of bijzondere persoonsgegevens van een individu |
|  | Organisatie | Grote financiële gevolgen (>€100.000) | Stevige imagoschade |
|  | Maatschappij | Lichte maatschappelijke onrust op grote schaal of grote maatschappelijke onrust op kleine schaal |
| 4 | Geraakte gegevens | Bijzondere en/of gevoelige gegevens van meerdere betrokkenen |
|  | Rechten betrokkene | Ernstige tot onherstelbare inbreuk op rechten en vrijheden van betrokkenen |
|  | Datalek | Verlies van gevoelige of bijzondere persoonsgegevens van meerdere betrokkenen |
|  | Organisatie | Faillissement of vergelijkbaar |
|  | Maatschappij | Grote maatschappelijke onrust op grote schaal |

Kans

|  |  |
| --- | --- |
| **Score** | **Kans** |
| 1 | <1 keer per jaar |
| 2 | Jaarlijks |
| 3 | Maandelijks |
| 4 | Wekelijks |

De tabel op de volgende pagina bevat de weergave van deze risico’s.

Wij adviseren om onderscheid te maken tussen de risicoscores op basis van de volgende verdeling:

|  |  |  |
| --- | --- | --- |
| Type risico | Risiconiveau | Acceptatiecriterium |
| Geen significant risico | Laag (1-4) | De <organisatie> treft **geen** additionele maatregelen. |
| Acceptabel risico | Middel (6-9) | De <organisatie> treft **mogelijk** additionele maatregelen. |
| Onacceptabel risico | Hoog (12-16) | De <organisatie> **moet** additionele maatregelen treffen om het risico naar minimaal een acceptabel niveau te mitigeren (score ≤ 9). |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Risicoanalyse: NAAM** | | | | | | | | | Restrisico | | |
| **NR** | **Categorie** | **Dreiging** | **Gegevensstromen** | **Omschrijving** | **K** | **I** | **R\*** | **Beoogde maatregel** | **K2** | **I3** | **R4** |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |

# Advies functionaris gegevensbescherming

In dit hoofdstuk plaatst de FG advies over de uitvoering van de DPIA en de maatregelen.

Indien voorafgaande raadpleging nodig is: <https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/voorafgaande-raadpleging>

# inbreng betrokkenen

<in de vorm van bijvoorbeeld: studentenraad / cliëntenraad / naastbetrokkenenraad / OR / etc.>

# procesverantwoordelijke

<Hier geeft de procesverantwoordelijke aan kennis te hebben genomen van de DPIA en verantwoordelijkheid te dragen over het uitvoeren van de mitigerende maatrelen.>

Datum: [ Datum ]

Naam procesverantwoordelijke: [ Naam ]

Functie procesverantwoordelijke: [ Functie ]

Ondertekening:

Tussenblad fase 2

**FASE 2**

# implementie van maatregelen

Aanpak

<Beschrijf hier welke maatregelen er worden opgepakt, en welke risico’s hiermee zullen worden gemitigeerd. Beschrijf of deze projectmatig of op een andere wijze worden opgepakt. Wijs eigenaren toe van de acties.>

DOORLOOPTIJD

Voor het doorvoeren van alle maatregelen voeren verwachten we een doorlooptijd van x maanden.

De doorlooptijd van project: <projectnaam> is naar verwachting x maanden.

De doorlooptijd van project: <projectnaam> is naar verwachting x maanden.

De verschillende projecten kunnen wel / niet / deels parallel worden uitgevoerd

KOSTEN

<kosten schatting per project>

Bijlage 1: geraadpleegde bronnen

1. <https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/praktisch-avg/data-protection-impact-assessment> [↑](#footnote-ref-2)