|  |  |
| --- | --- |
| Versie | 3.0 |
|  |  |
|  |  |
| Datum | 25 juli 2023 |
| Status  Contact | Definitief  Ministerie van BZK, Directie CIO Rijk  PAR - team: privacy-ciorijk@minbzk.nl |

Rapportagemodel DPIA Rijksdienst

**Vaststelling**

Verwerkingsverantwoordelijke: [Datum]

Naam: [Naam/Functie]

Advies functionaris voor gegevensbescherming: [Datum]

Naam: [Naam/Functie]

Versie: X

Status: Concept/Definitief

Revisie:

|  |  |  |
| --- | --- | --- |
| Versie | Datum | Toelichting |
| Versie 0.1 |  | Concept omschrijving voorstel, persoonsgegevens en gegevensverwerkingen. |
| Versie 0.2 |  | Verwerking feedback en eerste aanzet verwerkingsdoeleinden en betrokken partijen. |

**Inhoudsopgave**

[*Inleiding* 4](#_Toc142997931)

[*Managementsamenvatting* 5](#_Toc142997932)

[*Beschrijving kenmerken gegevensverwerkingen 6*](#_Toc142997933)

[1. Voorstel 7](#_Toc142997934)

[2. Persoonsgegevens 7](#_Toc142997935)

[3. Gegevensverwerkingen 8](#_Toc142997936)

[4. Technieken en methoden van de gegevensverwerkingen 8](#_Toc142997937)

[5. Verwerkingsdoeleinden 9](#_Toc142997938)

[6. Betrokken partijen 10](#_Toc142997939)

[7. Belangen bij de gegevensverwerkingen 10](#_Toc142997940)

[8. Verwerkingslocaties 11](#_Toc142997941)

[9. Juridisch en beleidsmatig kader 11](#_Toc142997942)

[10. Bewaartermijnen 12](#_Toc142997943)

[*Beoordeling rechtmatigheid gegevensverwerkingen* 13](#_Toc142997944)

[11. Rechtsgrond 14](#_Toc142997945)

[12. Bijzondere persoonsgegevens 15](#_Toc142997946)

[13. Doelbinding 16](#_Toc142997947)

[14. Noodzaak en evenredigheid 17](#_Toc142997948)

[15. Rechten van betrokkenen 18](#_Toc142997949)

[*Beschrijving en beoordeling risico’s voor de betrokkenen* 19](#_Toc142997950)

[16. Risico’s voor betrokkenen 20](#_Toc142997951)

[*Maatregelen en restrisico’s* 21](#_Toc142997952)

[17. Maatregelen 22](#_Toc142997953)

[*Ondertekening* 23](#_Toc142997954)

# Inleiding

Dit is het rapportagemodel van het Rijksmodel DPIA. Een DPIA wordt uitgevoerd door de 17 paragrafen in de navolgende pagina’s zo helder en nauwkeurig mogelijk in te vullen en te beschrijven.

Dit rapportagemodel staat niet op zichzelf. Het is aan te raden om het Rijksmodel DPIA (delen I tot en met III) bij de hand te houden bij het schrijven van een DPIA. Met name deel III, de toelichting, is van belang bij het schrijven van de DPIA. Hierin wordt per paragraaf beschreven wat wordt verwacht qua invulling van desbetreffende onderdeel. Ook worden definities uitgebreid uitgelegd en worden handige voorbeelden gegeven.

Het Rijksmodel DPIA is [hier](https://www.kcbr.nl/beleid-en-regelgeving-ontwikkelen/beleidskompas/achtergrond-beleidskompas/verplichte-kwaliteitseisen/data-protection-impact-assessment) te vinden.

Voeg hier wanneer gewenst een openingsalinea of inleiding toe.

Denk bijvoorbeeld aan:

* Verwijzing naar het privacybeleid
* Motivatie achter de uitvoering van deze DPIA
* Informatie over de manier waarop deze DPIA is opgesteld

# Managementsamenvatting

[Voeg hier de managementsamenvatting toe na afronding rapportagemodel. De managementsamenvatting dient de belangrijkste punten te omvatten van de DPIA-rapportage, met name de geïdentificeerde risico’s en (voorgenomen) maatregelen om de risico’s te mitigeren]

# Beschrijving kenmerken gegevensverwerkingen

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

Onder A wordt de eerste stap beschreven van de DPIA: een overzicht van alle relevante feiten van de voorgenomen gegevensverwerkingen. Essentieel is dat de feiten helder en volledig zijn, want het resterende deel van de DPIA is gebaseerd op wat in dit onderdeel is beschreven.

# Voorstel

Beschrijf het voorstel waar de DPIA op toeziet op

[hoofdlijnen](#Hoofdlijnen_Mouseover" \o "Ter controle of het voorstel compleet is kunnen de volgende punten worden nagegaan:- Wat is de aanleiding van het voorstel- Vervangt of vernieuwt het voorstel een bestaande situatie en is deze situatie beschreven- Is bij het voorstel sprake van privacy by design en privacy by default en hoe heeft dat plaatsgevonden- wat zijn de redenen dat het voorstel op deze manier tot stand is gekomen) en benoem hoe het voorstel tot stand is gekomen en wat de beweegredenen zijn achter de totstandkoming van het voorstel.

*Beschrijf het voorstel hier tussen de lijnen*

# Persoonsgegevens

Beschrijf alle

[persoonsgegevens](#Persoonsgegevens_Mouseover" \o "Persoonsgegevens zijn alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Om te bepalen of iemand identificeerbaar is, dient rekening gehouden te worden met alle middelen waarvan redelijkerwijs valt te verwachten dat die kunnen worden gebruikt om de persoon te identificeren.Voorbeelden zijn:- Contactgegevens (e-mailadres, huisadres, telefoonnummer)- Demografische gegevens (leeftijd, geboortedatum, geslacht, nationaliteit, opleiding)- Apparaat- en internetgegevens (IP-adres, MAC-adres, metadata)- Financiële gegevens (Bankrekeningnummer, salaris, loonschaal, kredietwaardigheid)) die worden verwerkt. Classificeer deze persoonsgegevens naar: gewoon,

[gevoelig](#Gevoelig_Mouseover" \o "Dit zijn gegevens die niet wettelijk anders worden behandeld, maar wel een groter privacy risico met zich meebrengen dan gewone persoonsgegevens.Voorbeelden hiervan zijn:- gegevens over de financiële situatie van de betrokkene- gegevens die betrekking hebben op kwetsbare groepen, zoals kinderen of minderheden- gegevens die kunnen worden misbruikt voor (identiteits)fraude- communicatie- en locatiegegevens),

[bijzonder](#Bijzonder_Mouseover" \o "Bijzondere persoonsgegevens zijn in beginsel verboden om te verwerken. Er dient een uitzonderingsgrond van toepassing te zijn, voordat verwerking van bijzondere persoonsgegevens is toegestaan.Bijzondere persoonsgegevens zijn gegevens die iets zeggen over:- ras of etnische afkomst- politieke opvattingen- religieuze of levensbeschouwelijke overtuigingen- vakbondslidmaatschap- genetische gegevens- biometrische gegevens met het oog op unieke identificatie van de betrokkene- gezondheidsgegevens- gegevens over seksueel gedrag of seksuele gerichtheid),

[strafrechtelijk](#Strafrechtelijk_Mouseover2" \o " Definitie strafrechtelijke persoonsgegevens:Dit zijn persoonsgegevens die strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen betreffen. Verder gaat het ook om persoonsgegevens over een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag.) en wettelijk identificatienummer. Geef per categorie [persoonsgegev](#Betrokkenen_Mouseover)ens aan welke persoonsgegevens worden verzameld en geef aan wat de bron is van deze persoonsgegevens.

| Categorie betrokkenen | Categorie persoonsgegevens | Persoonsgegevens | Type persoons-gegeven (gewoon, gevoelig, bijzonder, strafrechtelijk, identificatie-nummer) | Bron |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

*Geef hier tussen de lijnen aanvullende informatie over de persoonsgegevens*

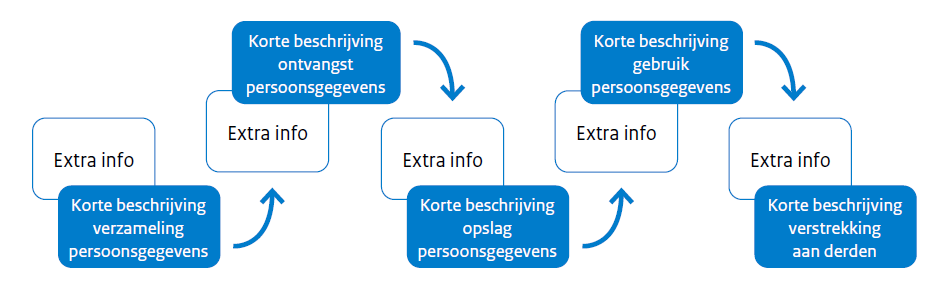
# Gegevensverwerkingen

Geef alle

[gegevensverwerkingen](#Verwerkingen_Mouseover" \o "Onder verwerking van persoonsgegevens wordt verstaan: elke bewerking of geheel van bewerkingen met betrekking tot persoonsgegevens. Oftewel, iedere handeling die met een persoonsgegevens plaatsvindt.Voorbeelden hiervan zijn: verzamelen, opslaan, wijzigen, raadplegen, verstrekken, combineren en verwijderen.) weer en geef aan welke categorieën persoonsgegevens worden verwerkt per gegevensverwerking. Desgewenst kan een stroomschema van de gegevensverwerkingen worden toegevoegd.

| Gegevensverwerking | Categorieën persoonsgegevens |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

*Geef hier tussen de lijnen aanvullende informatie over de gegevensverwerking*



Voorbeeld van een afbeelding dat de samenhang tussen gegevensverwerkingen laat zien.

# 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.

*Beschrijf hier tussen de lijnen de technieken en methoden van de gegevensverwerkingen.*

# Verwerkingsdoeleinden

Beschrijf de doeleinden van alle gegevensverwerkingen.

Voeg aanvullende informatie toe in het tekstveld.

| Gegevensverwerking | Verwerkingsdoeleinde | Oorspronkelijk verwerkingsdoeleinde |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

*Voeg tussen de lijnen aanvullende informatie toe over de verwerkingsdoeleinden.*

# Betrokken partijen

Benoem alle partijen die betrokken zijn en deel deze in per gegevensverwerking. Deel deze partijen in onder de rollen: [verwerkingsverantwoordelijke](#Verwerkingsverantwoordelijke_Mouseover" \o "De verwerkingsverantwoordelijke is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan, die het doel van en de middelen voor de gegevensverwerkingen vaststelt.),

[gezamenlijke verwerkingsverantwoordelijke](#Gezamenlijke_Mouseover" \o "Gezamenlijke verwerkingsverantwoordelijken zijn twee of meer verwerkingsverantwoordelijken die gezamenlijk de doeleinden en middelen van de verwerking bepalen. Deze partijen dienen onderling vast te leggen wie waarvoor verantwoordelijk en aansprakelijk is.),

[verwerker](#Verwerker_Mouseover" \o "Een verwerker is een natuurlijke persoon, rechtspersoon of het overheidsorgaan die voor de verwerkingsverantwoordelijke persoonsgegevens verwerkt.Partij is alleen verwerker voor zover de opdracht van de verwerkingsverantwoordelijke primair ziet op het verwerken van persoonsgegevens.),

[sub-verwerker](#Subverwerker_Mouseover" \o "Definitie sub-verwerker: De sub-verwerker is de natuurlijke persoon, rechtspersoon of het overheidsorgaan die primair de opdracht krijgt van de verwerker om persoonsgegevens te verwerken. De sub-verwerker wordt ook wel een onderaannemer genoemd.Voorbeeld van een sub-verwerker is de hostingpartij van de verwerker.),

[verstrekker](#Verstrekker_Mouseover" \o "Verstrekker is een natuurlijke persoon, organisatie of overheidsorgaan die persoonsgegevens doorgeeft aan een andere natuurlijke persoon, organisatie of overheidsorgaan.De rol van verstrekker kan overlappen met andere rollen die hier worden genoemd. Een organisatie kan, bijvoorbeeld, tegelijkertijd verwerkingsverantwoordelijke en verstrekker zijn.),

[ontvanger](#Ontvanger_Mouseover" \o "Ontvanger is een natuurlijke persoon, organisatie of overheidsogaan die persoonsgegevens ontvangt van een natuurlijke persoon, organisatie of overheidsorgaan.De rol van ontvanger kan overlappen met andere rollen die hier worden genoemd. Een organisatie kan, bijvoorbeeld, tegelijkertijd verwerker en ontvanger zijn.), [betrokkene(n)](#Betrokkenen_Mouseover) en [derde](#Derde_Mouseover" \o "Derde is een en  natuurlijke  persoon  of  rechtspersoon,  een overheidsinstantie,  een  dienst  of  een  ander  orgaan,  niet zijnde  de  betrokkene,  noch de  verwerkingsverantwoordelijke,  noch  de  verwerker,  noch  de  personen  die  onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken.;). 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 |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

*Voeg tussen de lijnen aanvullende informatie toe over de betrokken partijen.*

# 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 |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

*Voeg tussen de lijnen aanvullende informatie toe over de belangen*

# Verwerkingslocaties

Benoem in welke landen de gegevensverwerkingen plaatsvinden. Beschrijf het doorgiftemechanisme dat van toepassing is wanneer verwerkingslocaties buiten de Europese Economische Ruimte bevinden en noem of en welke aanvullende maatregelen van toepassing zijn. Voeg aanvullende informatie toe in het tekstveld.

*Zie deel III van het Rijksmodel DPIA voor meer informatie over de doorgiftemechanismen.*

| Gegevensverwerkingen | Verwerkingslocaties | Doorgiftemechanisme | Maatregelen |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

*Voeg hier tussen de lijnen aanvullende informatie over de verwerkingslocaties toe.*

# Juridisch en beleidsmatig kader

Benoem alle

[wet- en regelgeving](#Wetgeving_Mouseover" \o "Voorbeelden wet- en regelgeving. Hier is een lijst van voorbeelden van dergelijke wetten. Deze lijst is niet uitputtend:•Wet algemene bepalingen burgerservicenummer, •Wet gebruik burgerservicenummer in de zorg, •Wet basisregistratie personen, •Algemene wet inzake rijksbelastingen, •Archiefwet, •Telecommunicatiewet, •Kadasterwet, •Handelsregisterwet 2007, •Kieswet, •Wet bijzondere maatregelen grootstedelijke problematiek, •Wet op de geneeskundige behandelingsovereenkomst, Omgevingswet, •Jeugdwet, •Wet maatschappelijke ondersteuning 2015, en •Participatiewet.) en beleid met mogelijke gevolgen voor de gegevensverwerkingen. De AVG en de Richtlijn[[1]](#footnote-1) hoeven niet genoemd te worden. Voeg aanvullende informatie toe in het tekstveld.

| Gegevensverwerkingen | Juridisch en/of beleidsmatig kader | Wetsartikelen |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

*Voeg hier tussen de lijnen aanvullende informatie toe over het juridische en beleidsmatig kader toe.*

# 

# Bewaartermijnen

Bepaal de [bewaartermijnen](#Bewaartermijn_Mouseover" \o "De beschrijving van de bewaartermijn bestaat uit de 'ingang' van de bewaartermijn, de 'termijn' van de bewaartermijn en wat na de termijn moet gebeuren. Bijvoorbeeld: 2 jaar na einde arbeidsovereenkomst worden de persoonsgegevens geanonimiseerd en gearchiveerd. ) 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.

| Gegevens-verwerking | Verwerkings-doeleinde | Categorie Persoons-gegevens | Bewaartermijn | Motivatie bewaar-termijn |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

*Voeg hier tussen de lijnen aanvullende informatie over de bewaartermijnen toe.*

# Beoordeling rechtmatigheid gegevensverwerkingen

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

# 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.

De rechtsgronden zijn:

* Toestemming
  + Voor toestemming is nodig dat deze op ondubbelzinnige wijze vrij wordt gegeven voor een specifieke verwerking.

Licht toe hoe hieraan wordt voldaan.

* Noodzakelijk voor de uitvoering van de overeenkomst
  + Hier moet sprake zijn van een overeenkomst met de betrokkene, geef aan van wat voor overeenkomst sprake is.
* Noodzakelijk om te voldoen aan een wettelijke verplichting
  + Geef aan welke EU- of Nederlandse wetsbepalingen van toepassing zijn.
* Noodzakelijk om de vitale belangen van de betrokkene of een ander te beschermen
  + Hiervan kan sprake zijn wanneer iemands leven of gezondheid in gevaar is en die persoon niet in staat is om toestemming te geven.
* Noodzakelijk voor de vervulling van een taak van algemeen belang
  + Geef aan welke EU- of Nederlandse wetsbepalingen van toepassing zijn.
* Noodzakelijk voor de behartiging van een gerechtvaardigd belang
  + Deze grondslag is niet van toepassing op gegevensverwerkingen die worden uitgevoerd in het kader van de publieke taak van een overheidsorgaan.
  + Voor deze grondslag is een belangenafweging nodig, voeg deze toe aan de toelichting op de rechtsgrond.

| Gegevensverwerking | Rechtsgrond | Toelichting op de rechtsgrond |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

*Voeg hier tussen de lijnen aanvullende informatie over de rechtsgronden toe.*

# Bijzondere persoonsgegevens

Het verwerken van

[bijzondere](#Bijzonder_Mouseover2" \o "Bijzondere persoonsgegevens zijn in beginsel verboden om te verwerken. Er dient een uitzonderingsgrond van toepassing te zijn, voordat verwerking van bijzondere persoonsgegevens is toegestaan.Bijzondere persoonsgegevens zijn gegevens die iets zeggen over:- ras of etnische afkomst- politieke opvattingen- religieuze of levensbeschouwelijke overtuigingen- vakbondslidmaatschap- genetische gegevens- biometrische gegevens met het oog op unieke identificatie van de betrokkene- gezondheidsgegevens- gegevens over seksueel gedrag of seksuele gerichtheid) of

[strafrechtelijke](#Strafrechtelijk_Mouseover" \o "Strafrechtelijke persoonsgegevens zijn persoonsgegevens die strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen betreffen. Verder gaat het ook om persoonsgegevens over een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag.) persoonsgegevens is in principe verboden. Verwerking is pas mogelijk wanneer een

[uitzonderingsgrond](#Uitzonderingsgrond_Mouseover" \o "De uitzonderingsgronden zijn:- Uitdrukkelijke toestemming van de betrokkene.- Noodzakelijk voor de uitvoering van specifieke rechten of verplichtingen op grond van het arbeidsrecht of het sociale zekerheidsrecht, voor zover toegestaan bij EU- of Nederlands recht.- Noodzakelijk voor de bescherming van de vitale belangen van de betrokkene of een andere natuurlijke persoon, indien fysiek of juridisch niet in staat om toestemming te geven.- Verwerking wordt verricht door een stichting, vereniging of een andere instantie zonder winstoogmerk die werkzaam is op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied.- Verwerking gaat over persoonsgegevens die reeds openbaar zijn gemaakt.- Noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvorering.- Noodzakelijk vanwege een zwaarwegend algemeen belang op grond van EU- of Nederlands recht.- Noodzakelijk voor preventieve geneeeskunde, arbeidsgeneeskunde, beoordeling arbeidsgeschiktheid, medische diagnosen, verstrekken van gezondheidszorg of sociale diensten, het beheren van gezondheidszorgstelsels- en diensten, op grond van EU- of Nederlands recht of op grond van een overeenkomst met een gezondheidswerker.- Noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid, op grond van EU- of Nederlands recht.- Noodzakelijk met het oog op archivering van algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, op grond van EU- of Nederlands recht.) van toepassing is. Beoordeel of een van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een nationaal identificatienummer, beoordeel of dit is toegestaan.

Voeg aanvullende informatie toe in het tekstveld.

| Gegevensverwerking | Type bijzonder persoonsgegeven | Uitzonderingsgrond |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

*Voeg hier tussen de lijnen aanvullende informatie over de bijzondere persoonsgegevens toe.*

# 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

[verenigbaar](#Verenigbaar_Mouseover" \o "Ter beoordeling van de verenigbaarheid moet worden gekeken naar een aantal elementen:- het verband tussen het nieuwe doel en het oorspronkelijke doel. Hoe dichter die bij elkaar liggen, hoe eerder de verwerking verenigbaar is.- de context waarin de persoonsgegevens zijn verzameld. Hier moet worden gekeken naar de relatie tussen de verwerkingsverantwoordelijke en de betrokkene en wat de betrokkene redelijk kan verwachten.- de aard van de persoonsgegevens. Bij gevoelige persoonsgegevens geldt een hoger beschermingsniveau en dat deze minder snel voor andere doelen mogen worden gebruikt.- de mogelijke gevolgen van de verdere verwerking voor betrokkenen.- het bestaan van passende waarborgen. Wanneer de persoonsgegevens bijvoorbeeld zijn versleuteld of gepseudonimiseerd, zullen deze eerder voor andere doelen mogen worden gebruikt.) 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 |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

*Voeg hier tussen de lijnen aanvullende informatie over de doelbinding toe.*

# 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:

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

*Voeg hier tussen de lijnen de beoordeling van de proportionaliteit toe.*

*Voeg hier tussen de lijnen de beoordeling van de subsidiariteit toe.*

# Rechten van betrokkenen

Beschrijf de procedure waarmee invulling wordt gegeven aan de

[rechten van de betrokkenen](#Rechten_Mouseover" \o "Rechten van betrokkenen zijn:- Recht op informatie- Recht van inzage- Recht op rectificatie- Recht op gegevenswissing- Recht op beperking van de verwerking- Recht op beperking van de verwerking- Kennisgevingsplicht over rectificatie of wissing van persoonsgegevens- Recht op overdraagbaarheid van gegevens- Recht van bezwaarRecht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit) 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 |  |  |
| Recht op rectificatie en aanvulling |  |  |
| Recht op vergetelheid |  |  |
| Recht op beperking van de verwerking |  |  |
| Recht op dataportabiliteit |  |  |
| Recht niet onderworpen te worden aan geautomatiseerde besluitvorming |  |  |
| Recht om bezwaar te maken |  |  |
| Recht op duidelijke informatie |  |  |

*Geef een beschrijving hier tussen de lijnen.*

# Beschrijving en beoordeling risico’s voor de betrokkenen

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

# 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:

1. welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen, zoals het verbod op discriminatie;
2. de oorsprong van deze gevolgen;
3. de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;
4. 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.

De risicomatrix bestaat uit de eerdergenoemde drie risiconiveau's: laag, gemiddeld en hoog. Wanneer de kans laag is, is er sprake van een laag risico. Wanneer de impact laag is, is er eveneens sprake van een laag risico. Wanneer zoals de kans als de impact 'midden' is, is het risico eveneens 'gemiddeld'. Bij een hoge kans, en minimaal een gemiddelde impact (en andersom), is het risico hoog. 

\*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.

Voeg aanvullende informatie in het tekstveld toe.

| Beschrijving risico | Kans | Impact | Risico-inschatting |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

*Voeg hier tussen de lijnen aanvullende informatie over de risico’s toe.*

# Maatregelen en restrisico’s

In onderdeel D wordt bezien welke maatregelen kunnen worden getroffen om de in onderdeel C erkende risico’s te voorkomen of te verminderen.

Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de wetgever of verwerkingsverantwoordelijke. Voor dit onderdeel van de DPIA is in het bijzonder expertise over informatiebeveiliging belangrijk.

# Maatregelen

Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico’s te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt. Voeg aanvullende informatie in het tekstveld onder de tabellen toe.

Beschrijf ook de resterende risico’s die nog aanwezig zijn na de uitvoering en/of implementatie van de geïdentificeerde maatregelen. Geef per resterend risico aan wat het niveau is van dit risico.

Geef tot slot een conclusie over de restrisico’s. Zijn deze acceptabel? En is er een voorafgaande raadpleging bij de Autoriteit Persoonsgegevens nodig?

Gebruik voor de inschattingen van de risico’s de niveaus ‘laag’, ‘gemiddeld’ en ‘hoog’. Gebruikmaken van de bijbehorende kleuren is aan te raden.

| Risico | Maatregelen | Resterend risico en risico-inschatting | Beheerder van maatregelen |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

*Voeg hier tussen de lijnen aanvullende informatie over de maatregelen toe.*

*Voeg hier tussen de lijnen de beschrijving toe over de resterende risico’s, de risico-inschatting en onderbouwing voor acceptatie resterende risico’s. Noem ook of er een voorafgaande raadpleging nodig is of niet.*

# Ondertekening

Om de DPIA formeel vast te stellen is het noodzakelijk deze te ondertekenen, zodat het duidelijk is dat de DPIA door de verantwoordelijke(n) akkoord is bevonden.

|  |  |
| --- | --- |
| Naam verantwoordelijke(n) |  |
| Directie/afdeling verantwoordelijke(n) |  |
| Functie verantwoordelijke(n) |  |
| Datum ondertekening |  |
| Handtekening |  |

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. [↑](#footnote-ref-1)