|  |
| --- |
|  |
| **Format DPIA-rapportage DGC** |
| Geschikt voor de DPIA-rapportage van kwaliteitsregistraties |

Afbeelding met persoon

Automatisch gegenereerde beschrijving

Het format DPIA-rapportage DGC is in beheer bij het Shared Service Center Data Governance (SSC-DG). Op [www.ssc-dg.nl](http://www.ssc-dg.nl) vindt u altijd de meest recente versie.

Versie: 1.0, 23 juli 2025

Vertrouwelijkheid: openbaar

Aparte bijlage bij dit document: Verantwoordingstabel v1.0 (Excel-bestand)

**Inhoudsopgave**

[Deel 1: Verantwoording en instructies 3](#_Toc203489610)

[Deel 2: DPIA-rapportage 5](#_Toc203489611)

[A. Beschrijving kenmerken gegevensverwerkingen 6](#_Toc203489612)

[**1.** **Voorstel gegevensverwerking** 6](#_Toc203489613)

[**2.** **Persoonsgegevens** 7](#_Toc203489614)

[**3.** **Gegevensverwerkingen** 8](#_Toc203489615)

[**4.** **Technieken en methoden van de gegevensverwerking(en)** 9](#_Toc203489616)

[**5.** **Verwerkingsdoeleinden** 11](#_Toc203489617)

[**6.** **Betrokken partijen** 12](#_Toc203489618)

[**7.** **Belangen bij de gegevensverwerking** 13](#_Toc203489619)

[**8.** **Verwerkingslocaties** 14](#_Toc203489620)

[**9.** **Juridisch en beleidsmatig kader** 15](#_Toc203489621)

[**10.** **Bewaartermijnen** 15](#_Toc203489622)

[B. Beoordeling rechtmatigheid gegevensverwerking 16](#_Toc203489623)

[**11.** **Rechtsgrond** 16](#_Toc203489624)

[**12.** **Bijzondere persoonsgegevens** 16](#_Toc203489625)

[**13.** **Doelbinding** 18](#_Toc203489626)

[**14.** **Noodzaak en evenredigheid** 19](#_Toc203489627)

[**15.** **Rechten van betrokkenen** 19](#_Toc203489628)

[C. Beschrijving en beoordeling risico’s voor de betrokkenen 21](#_Toc203489629)

[**16.** **Risico’s voor betrokkenen** 21](#_Toc203489630)

[D. Beschrijving voorgenomen maatregelen 23](#_Toc203489631)

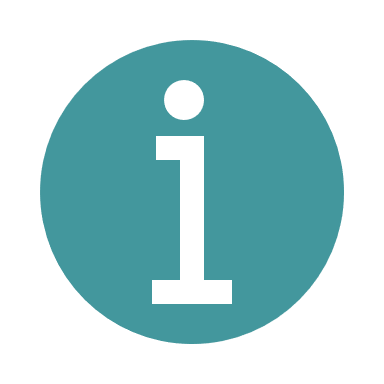
[**17.** **Maatregelen** 23](#_Toc203489632)

Conclusie en [ondertekening 25](#_Toc203489633)

# Deel 1: Verantwoording en instructies

Voor u ligt het format DPIA-rapportage DGC. Dit document is op verzoek van de Data-governancecommissie (DGC) opgesteld, in afstemming met de door het Shared Service Center Data Governance (SSC-DG) opgezette expertgroep ‘Onafhankelijke toets DPIA’.

Het doel van een DPIA (data protection impact assessment) is het in kaart brengen van mogelijke privacyrisico’s van een gegevensverwerking, zodat de verwerkingsverantwoordelijke (hier: de registratiehouder) passende maatregelen kan nemen om deze risico’s te verkleinen. Aan registratiehouders wordt verzocht bij het uitvoeren van hun DPIA gebruik te maken van dit format. Daarvoor gebruikt u **deel 2** van dit document.

 Het uitvoeren van een DPIA is een voorwaarde voor opname in het landelijk register voor kwaliteitsregistraties, volgens artikel 11o, lid 1 sub g Wkkgz. Tevens is het verplicht om een DPIA uit te voeren wanneer een verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen (volgens artikel 35 AVG). Bij de beoordeling hiervan dient volgens de EDPB (European Data Protection Board) o.a. in aanmerking te worden genomen of het gevoelige gegevens/gegevens van zeer persoonlijke aard betreft, of het om verwerken op grote schaal gaat en of er eventueel datasets worden samengevoegd.[[1]](#footnote-2)

**Opbouw DPIA-rapportage**

Dit format voor de DPIA-rapportage is rechtstreeks afgeleid van het Model DPIA Rijksdienst (binnen de overheid gebruikt om hoog-risico verwerkingen van persoonsgegevens te beoordelen). De rapportage bestaat (net als het model) uit 17 punten verspreid over vier onderdelen:

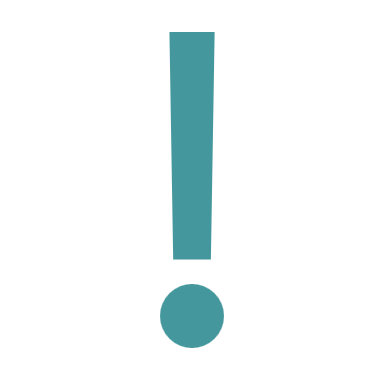
* Onderdeel A behelst de beschrijving van de gegevensverwerking.
* Onderdeel B beoordeelt op basis van de relevante wet- en regelgeving de rechtmatigheid van de beschrijving uit onderdeel A.
* Onderdeel C gaat over risico’s voor de rechten en vrijheden van betrokkenen.
* Onderdeel D gaat over de beoogde maatregelen om die risico’s aan te pakken.

De beantwoording van de 17 punten kan meer of minder gedetailleerd zijn, afhankelijk van de aard en omvang van de regelgeving of verwerkingen. Wel is het in alle gevallen noodzakelijk om alle punten na te gaan en de gemaakte afwegingen per punt op te schrijven.

**Instructies en tekstsuggesties**

Gestreefd is naar een zo goed mogelijke ondersteuning van de registratiehouders bij het uitvoeren van hun DPIA. Dit format bevat daarom per onderdeel instructies en tekstsuggesties, en eventueel aanvullende informatie.

Er zijn tekstsuggesties opgenomen voor de onderdelen waarvan wordt verwacht dat deze voor veel kwaliteitsregistraties/registratiehouders hetzelfde zullen zijn. Bij (veel) kwaliteitsregistraties is er namelijk sprake van een gelijksoortige verwerking: een grootschalige verwerking van gezondheidsgegevens ten behoeve van het voeren van een kwaliteitsregistratie, (doorgaans) gebaseerd op hetzelfde wettelijk kader.

Het opleveren (en bijwerken) van een volledige en accurate DPIA-rapportage is de verantwoordelijkheid van de registratiehouder. Alle vooraf ingevulde tekstsuggesties kunnen worden gebruikt, maar het is de verantwoordelijkheid van de registratiehouder om de inhoud te verifiëren en waar mogelijk aan te passen, aan te vullen en/of te herschrijven zodat de tekst passend is voor de kwaliteitsregistratie.

**Dynamisch proces**

De DGC hecht eraan te benadrukken dat het uitvoeren van een DPIA een dynamisch proces is, dat door middel van de DPIA-rapportage in beeld wordt gebracht. Het is aannemelijk dat bij het beoordelen van de privacyrisico’s in onderdeel C en de maatregelen in onderdeel D, de gegevensverwerkingen in de praktijk gewijzigd dienen te worden, bijvoorbeeld omdat de beoordeelde risico’s toch te groot blijken te zijn. Wanneer de gegevensverwerkingen n.a.v. deze uitkomsten in de praktijk zijn gewijzigd, dan dienen de punten uit onderdeel A en B ook gewijzigd te worden om de realiteit te reflecteren. De registratiehouder stelt hiervoor een PDCA-cyclus in.

# Deel 2: DPIA-rapportage

**DPIA-rapportage Naam kwaliteitsregistratie**

**Vaststelling**

**Verwerkingsverantwoordelijke registratiehouder:**

Naam organisatie:

**Functionaris voor de gegevensbescherming (van registratiehouder):**

Naam:

**Aan deze DPIA hebben meegewerkt:**

Naam en functie:

Naam en functie:

Naam en functie:

**Versie:** X.X

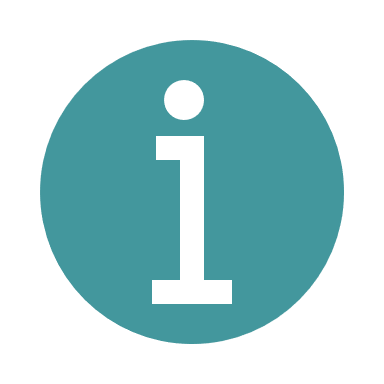
**Status:** Concept/Definitief

**Versiebeheer**

|  |  |  |
| --- | --- | --- |
| Versienummer | Datum | Toelichting |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

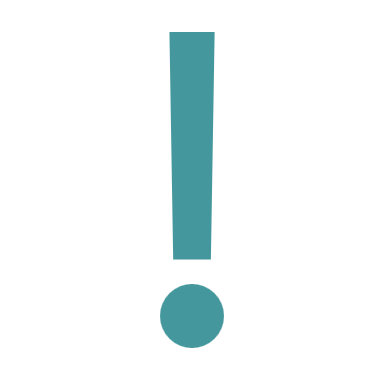
## Beschrijving kenmerken gegevensverwerkingen

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

 Onder A wordt de eerste stap beschreven van de DPIA: een overzicht van de relevante feiten van de voorgenomen gegevensverwerking(en). Als de feiten onduidelijk zijn, werkt dit door in de beoordeling.

### **Voorstel gegevensverwerking**

Beschrijf de gegevensverwerking waar de DPIA op toeziet en benoem hoe het voorstel tot stand is gekomen en wat de beweegredenen zijn achter de totstandkoming van het voorstel. Specifiek betekent dit: Beschrijf kort (op hoofdlijnen) de aandoening, ziekte, zorgtype of complicatie, of combinaties daarvan en beschrijf duidelijk de inclusie- en eventuele exclusiecriteria van patiënten die in de registratie opgenomen moeten worden.

Het is uitdrukkelijk niet de bedoeling dat de registratiehouder gegevens verzamelt met als primair doel het uitvoeren van wetenschappelijk onderzoek. Tevens is het de registratiehouder (als verwerkingsverantwoordelijke) niet toegestaan om de (gepseudonimiseerde) persoonsgegevens aan derden te verstrekken voor het doen van wetenschappelijk onderzoek.

*\* Tekstsuggestie \**

Doel van de Naam kwaliteitsregistratie is het continu meten en verbeteren van de kwaliteit van medisch specialistische zorg aan patiënten/cliënten die gekenmerkt worden door …

Om dit doel te bereiken worden gepseudonimiseerde persoonsgegevens[[2]](#footnote-3), waaronder bijzondere persoonsgegevens, van deze gedefinieerde patiënten/cliëntenpopulatie verzameld, opgeslagen en verder verwerkt. Op basis van analyses van en benchmarkrapportages over de kwaliteit van de geleverde zorg, kunnen zorgverleners en zorgaanbieders van elkaar leren en zo de kwaliteit van zorg verbeteren. De kwaliteitsregistraties dienen daarmee een algemeen belang ter borging en verbetering van de kwaliteit van zorg.

[Optioneel] Naam registratiehouder gebruikt deze gegevens bovendien zelf voor het doen van onderzoek, om zo het meetinstrument of de dataset door te ontwikkelen. Het gebruik van gegevens voor het doen van onderzoek door de registratiehouder is verenigbaar met de oorspronkelijke doeleinden op grond van artikel 5 lid 1 sub b AVG.

### **Persoonsgegevens**

Benoem de inclusiecriteria van de kwaliteitsregistratie en vul de verantwoordingstabel in (bijlage 1, Excel-bestand). Hierin onderbouwt u welke (gepseudonimiseerde) persoonsgegevens noodzakelijk zijn voor de doelen van de kwaliteitsregistratie. Som daarna (in de tabel) alle categorieën van (gepseudonimiseerde) persoonsgegevens op die worden verwerkt. Geef per categorie van aan op wie de gegevens betrekking hebben. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder en wettelijk identificerend.

*\* Tekstsuggestie \**

Een registratiehouder mag op basis van artikel 11p Wkkgz zowel bijzondere als niet bijzondere (gepseudonimiseerde) persoonsgegevens verwerken, voor zover dit noodzakelijk is om de kwaliteit van zorg aan de cliëntenpopulatie waarop de betreffende kwaliteitsregistratie ziet te meten en te verbeteren.

De Naam kwaliteitsregistratie bevat informatie over personen die voldoen aan de inclusiecriteria. Een uitgebreide omschrijving van de inclusiecriteria is opgenomen in de data dictionary van de Naam kwaliteitsregistratie. Deze is hier te vinden: url.

Naam registratiehouder heeft in bijgevoegde verantwoordingstabel onderbouwd welke (gepseudonimiseerde) persoonsgegevens noodzakelijk zijn voor de doelen van de kwaliteitsregistratie.

Voor Naam kwaliteitsregistratie betreft het de volgende categorieën van gegevens (afgeleid van de verantwoordingstabel):

|  |  |  |
| --- | --- | --- |
| Categorie  gegevens | Typering persoonsgegeven | Relevantie |
| BSN\* | Het Burgerservicenummer. *Wettelijk identificerend*. | BSN wordt gebruikt voor het (deterministisch) koppelen van gegevens uit diverse bronnen (verstrekkers). |
| UPN | Uniek patiëntnummer (identificatie) van een persoon in het elektronisch patiëntendossier bij de betreffende zorgaanbieder.  *Bijzonder persoonsgegeven*. | Variabele waarmee patiënten door de zorgaanbieder uniek geïdentificeerd kunnen worden voor kwaliteitsbewaking- en verbetering en terugkoppeling. |
| Geslacht | *Gewoon persoonsgegeven.* | Variabele voor het realiseren van output/statistieken en voor het maken van koppelingen. |
| Geboortedatum | *Gewoon persoonsgegeven.* | Variabele voor het realiseren van output/statistieken en voor het maken van koppelingen. |
| Geboortenaam | *Gewoon persoonsgegeven*. | Variabele benodigd voor het maken van koppelingen. |
| Zorgspecifieke BASIS-gegevens | *Bijzondere persoonsgegevens.* | BASIS-gegevens gericht op leren en verbeteren en samen beslissen.  De exacte gegevensset wordt jaarlijks vastgesteld en gepubliceerd (data dictionary) op de website van de registratiehouder en nader beschreven in de verantwoordingstabel.  De BASIS-gegevensset dient door álle zorgaanbieders die deze zorg leveren aan registratiehouder verstrekt te worden. Er kan hierbij sprake zijn van een benodigd onderscheid in aan te leveren data op basis van de zorg die geleverd wordt per categorie zorgaanbieders. |
| Zorgspecifieke PLUS-gegevens | *Bijzondere persoonsgegevens.* | PLUS -gegevens die gebruikt worden voor het dóórontwikkelen van het meetinstrument.  De exacte PLUS-gegevensset wordt jaarlijks vastgesteld en herkenbaar als PLUS-dataset gepubliceerd (data dictionary) op de website van de registratiehouder en nader beschreven in de verantwoordingstabel.  Aanleveren kan verplicht worden voor een bepaalde subset van zorgaanbieders. |
| Etniciteit | *Bijzondere persoonsgegevens.* | Etniciteit is noodzakelijk voor casemixcorrectie:   * bij het evalueren van behandelingen waarvan bekend is dat de effectiviteit etnisch kan verschillen (bijv. bepaalde medicijnen). * bij het trekken van de juiste conclusies indien uit eerdere analyses/literatuur blijkt dat etniciteit een significante invloed heeft op zorguitkomsten. |

*\* Let op dat voor het verwerken van het (gepseudonimiseerde) BSN altijd een expliciete wettelijke grondslag nodig is. Zo’n grondslag is er bijvoorbeeld voor de LTR en LADIS.*

### **Gegevensverwerkingen**

Geef alle gegevensverwerkingen weer en geef aan welke categorieën persoonsgegevens worden verwerkt per gegevensverwerking. Het wordt aanbevolen een stroomschema van de gegevensverwerkingen toe te voegen.

*\*Tekstsuggestie\**

De verwerkingen van gepseudonimiseerde persoonsgegevens die in het kader van deze kwaliteitsregistratie door registratiehouder worden gedaan bestaan uit:

1. Gegevensontvangst door Naam registratiehouder, evt. wel via zijn verwerker(s)
2. [Optioneel] Het koppelen van gegevens uit diverse bronnen
3. Het uitvoeren van de kwaliteitsmetingen en het publiceren van de benchmark
4. Onderzoek in het kader van beheren en onderhouden van de dataset.
5. Onderzoek in het kader van dóórontwikkeling van de kwaliteitsregistratie.

De publicaties van de benchmarkresultaten en publicaties die volgen uit de onderzoeken bevatten géén persoonsgegevens meer. Naam registratiehouder voert hiertoe output controles uit op elke publicatie en te exporteren gegevensset.

**Een schematische weergave (stroomschema) van de gegevensverwerkingen:**

Voeg afbeelding in

**Ad 1. Gegevensontvangst door Naam registratiehouder, evt. via zijn verwerker(s)**

Naam registratiehouder ontvangt van zorgaanbieders de gepseudonimiseerde gegevens zoals bepaald in de data dictionary van de Naam kwaliteitsregistratie. De aanleverbestanden bevatten in principe alle gegevens, zoals gedefinieerd in de BASIS-gegevensset, van alle personen die voldoen aan de inclusiecriteria van de kwaliteitsregistraties.[[3]](#footnote-4)

[Optioneel] Voor de PLUS-gegevensset geldt dat die uitsluitend aangeleverd hoeft te worden voor een bepaalde subset van zorgaanbieders.

[Optioneel] **Ad 2. Het koppelen van gegevens uit diverse bronnen**

De gegevens die ten behoeve van de kwaliteitsregistratie verwerkt dienen te worden, worden door zorgaanbieders (en evt. andere bronhouders) gepseudonimiseerd aangeleverd, waarbij de betreffende zorgaanbieders ervoor zorgen dat de gegevens van een specifieke patiënt voorzien worden van éénzelfde pseudoniem. Naam registratiehouder kan op basis van dit pseudoniem de koppeling op patiëntniveau tot stand brengen tussen gegevens afkomstig uit de diverse bronnen.

**Ad 3. Het uitvoeren van de kwaliteitsmetingen en het publiceren van de benchmark**

Na het beschikbaar komen van de gepseudonimiseerde BASIS-gegevensset, verwerkt Naam registratiehouder de gegevens ten behoeve van de kwaliteitsmeting/benchmark. De BASIS-gegevensset wordt binnen de beveiligde netwerkomgeving van Naam registratiehouder of diens verwerker opgeslagen. Toegang tot de gegevens door medewerkers van Naam registratiehouder of diens verwerker is op basis van need-to-know en geïmplementeerd door een Authenticatie en Autorisatie systeem (IAM-systeem).

De BASIS-gegevensset wordt geanalyseerd en verwerkt tot indicatoren en statistieken die inzicht geven in de kwaliteit van de geleverde zorg. De analyseresultaten worden o.a. in benchmark rapporten/dashboards gepubliceerd.

**Ad 4. Onderzoek in het kader van beheren en onderhouden van de dataset**

Naam registratiehouder verwerkt de gegevens uit de BASIS-gegevensset in het kader van de PDCA-cyclus (*check*) ook ten behoeve van het beheer en onderhoud van de dataset.

**Ad 5. Onderzoek in het kader van dóórontwikkeling van de kwaliteitsregistratie**

Naam registratiehouder verwerkt de gegevens uit de PLUS-gegevensset in combinatie met de BASIS-gegevensset in het kader van de PDCA-cyclus (*plan*) ook ten behoeve van het dóórontwikkelen van de kwaliteitsregistratie.

### **Technieken en methoden van de gegevensverwerking(en)**

Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de (gepseudonimiseerde) persoonsgegevens worden verwerkt. Benoem, bijvoorbeeld, of sprake is van een cloudoplossing of big dataverwerkingen en, zo ja, beschrijf waaruit dat bestaat.

*\* Tekstsuggestie \**

**Algemeen**

Naam registratiehouder verwerkt alleen gegevens voor het meten en verbeteren van de kwaliteit van zorg aan de cliëntenpopulatie waarop de betreffende kwaliteitsregistratie betrekking heeft en het faciliteren van ‘samen beslissen’. Er is géén sprake van (semi-)geautomatiseerde besluitvorming of profilering. Bij publicatie zijn de gegevens nooit te herleiden naar één persoon.

**Gegevensontvangst**

1. Benoem de frequentie, techniek, bestandsformat, inhoud (alleen nieuwe patiënten, of ook mutaties aan bestaande patiënten) van aanlevering.
2. Onderwerpen die van belang kunnen zijn:
   1. Ontvangen
      1. API (REST, SOAP)
      2. ETL
      3. Handmatige uploads
      4. Etc.
   2. Validatie, authenticatie en autorisatie
   3. Preprocessing & kwaliteitscontrole
   4. Notificaties verstrekkers
   5. Transformatie, data cleaning, normalisatie
      1. Python
      2. R
      3. Codering/conversie
   6. Koppelen
   7. Logging & monitoring
   8. Versiebeheer & archivering
   9. Bewaartermijn aanleverbestanden

**Het uitvoeren van de kwaliteitsmetingen en het publiceren van de benchmark**

1. Staging
   1. Python
   2. R
   3. SQL
   4. Logging en monitoring
   5. Versiebeheer en bestandsregistratie
2. Analyseren en berekenen
   1. Formules en business rules (scripting)
   2. Groeperen/stratificeren en aggregeren
   3. Modelleren
   4. Python/R scripts
3. Benchmarkberekeningen
   1. Percentielen
   2. Ranking
   3. Statistische standaardisatie
   4. Peer group-indelingen
4. Visualisatie
   1. BI
   2. Dashboards met interactieve elementen
5. Publicatie en distributie
   1. Webportals
   2. API’s
   3. Anonimisering
6. Beheer
   1. Metadata management
   2. Logging
   3. Feedback mechanismen

**Het beschikbaar maken van de gegevens voor en/of het uitvoeren van statistisch en/of wetenschappelijk onderzoek**

1. Beoordelen
   1. Proces beoordelen en goedkeuren aanvraag onderzoek
      1. Ethische toetsing
      2. Compliance
2. Samenstellen dataset/data cleaning
   1. SQL-query
   2. API’s of data-exportmodule
   3. R
3. Pseudonimiseren/anonimiseren
4. Data documentatie
   1. Metadata codeboeken en data dictionaries
   2. Methodologische toelichting
5. Dataopslag en toegangsbeheer
   1. Beveiligde verwerkingsomgeving
   2. Twee factor authenticatie
   3. Rollen
6. Beheer en versiecontrole

### **Verwerkingsdoeleinden**

Beschrijf de doeleinden van de voorgenomen gegevensverwerking(en).

*\* Tekstsuggestie \**

Het doel van de verwerking van de gepseudonimiseerde persoonsgegevens die zorgaanbieders beschikbaar stellen aan Naam registratiehouder is het meten en verbeteren van de kwaliteit van zorg aan de cliëntenpopulatie waarop de betreffende kwaliteitsregistratie ziet (artikel 11p lid 1 Wkkgz). Deze wettelijke grondslag voor kwaliteitsregistraties geldt uitsluitend ten behoeve van de doelen ‘leren en verbeteren’ en ‘samen beslissen’.

### **Betrokken partijen**

Benoem welke organisaties betrokken zijn bij welke gegevensverwerking(en). 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.

*\* Tekstsuggestie \**

**Registratiehouder is verwerkingsverantwoordelijke**

Naam registratiehouder is op grond van artikel 11p Wkkgz verantwoordelijk voor het meten en verbeteren de kwaliteit van zorg van de cliëntenpopulatie waarop de Naam kwaliteitsregistratie betrekking heeft. Naam registratiehouder bepaalt de methode waarmee die kwaliteit gemeten wordt en of de uitkomsten van die metingen openbaar gemaakt worden. Naam registratiehouder is daarin onafhankelijk. Op grond van artikel 1 lid 1 Wkkgz is Naam Registratiehouder verwerkingsverantwoordelijk voor een in het register voor kwaliteitsregistraties opgenomen kwaliteitsregistratie. Ook is Naam registratiehouder ontvanger van de gepseudonimiseerde persoonsgegevens van zorgaanbieder.

**Verwerker**

Naam registratiehouder maakt ten behoeve van deze gegevensverwerking(en) gebruik van de volgende verwerker(s):

|  |  |  |  |
| --- | --- | --- | --- |
| Naam verwerker | Beschrijving diensten en persoonsgegevens | Gegevensverwerking  buiten de EER | Verwerkers-overeenkomst |
| <naam>  <adres>  <url> | <Omschrijving> | Ja/nee\* | Ja/nee |
|  |  |  |  |

*\* Indien ‘ja’, vermeld land en adequaatheidsbesluit of genomen passende maatregelen waaronder doorgifte plaatsvindt.*

**Verstrekkers**

Zorgaanbieders die zorg verlenen aan cliënten die overeenkomsten vertonen in hun aandoening, ziekte, zorgtype of complicatie, of combinaties daarvan én die voldoen aan de inclusiecriteria van de Naam kwaliteitsregistratie zijn op basis van artikel 11q lid 3 Wkkgz wettelijk verplicht de gegevens gepseudonimiseerd aan te leveren.

**Ontvangers**

Gegevens worden passend beschermd en beschikbaar gesteld aan (medewerkers van) Naam registratiehouder of diens verwerker(s) die belast zijn met uitvoeren van de kwaliteitsmeting.

### **Belangen bij de gegevensverwerking**

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

*\* Tekstsuggestie\**

**Belangen van betrokkenen**

1. Veiligere zorg  
   Door kwaliteit te meten worden fouten, incidenten of risico’s sneller opgespoord.
2. Betere behandeling en uitkomsten  
   Kwaliteitsmetingen brengen in kaart of behandelingen werken en wat de resultaten zijn.  
   Patiënten profiteren van zorg die voortdurend wordt verbeterd op basis van data.
3. Meer inspraak en transparantie  
   Als uit metingen blijkt waar het goed of minder goed gaat, kunnen patiënten bewust kiezen voor een zorgaanbieder.
4. Zorg op maat  
   Metingen kunnen ook inzicht geven in patiëntervaringen, wat leidt tot meer persoonsgerichte zorg.

**Belangen van zorgaanbieders**

1. Verbeteren van zorgprocessen  
   Metingen maken zichtbaar waar knelpunten zitten, zoals fouten, wachttijden of onnodige heropnames.  
   Daardoor kunnen processen efficiënter worden ingericht.
2. Kwaliteit aantonen aan buitenwereld  
   Zorgverzekeraars, inspectie (IGJ), patiënten en overheid willen zien hoe goed een zorgaanbieder het doet.  
   Kwaliteitscijfers helpen om vertrouwen te winnen en verantwoording af te leggen.
3. In gesprek gaan met professionals  
   Zorgverleners kunnen hun handelen spiegelen aan data: “Doen wij het goed?” of “Waarom wijken wij af?”  
   Dit stimuleert professionele reflectie en teamleren.
4. Sturen op uitkomsten i.p.v. enkel op processen  
   Kwaliteitsmetingen geven inzicht in de effectiviteit van zorg.  
   Hierdoor kan de zorg meer gericht worden op wat er écht toe doet voor de patiënt.
5. Financiering en contractering  
   Veel zorgverzekeraars koppelen contracten (en tarieven!) aan meetbare kwaliteit.  
   Denk aan "uitkomstgerichte zorg", waarbij goede prestaties beloond worden.
6. Risicomanagement en compliance  
   Vroegtijdig problemen signaleren voorkomt grotere incidenten of boetes.  
   Voldoen aan verplichtingen van IGJ, NZA, en AVG wordt makkelijker met structurele meting en rapportage.

Belangen van **Naam registratiehouder**

1. heeft geen direct belang bij de uitkomsten van de kwaliteitsmeting anders dan dat de meting op een kwalitatief juiste wijze uitgevoerd wordt.
2. Verzamelen van betrouwbare data voor kwaliteitsverbetering  
   Registratiehouders zorgen voor standaardisatie van gegevens: iedereen meet op dezelfde manier.  
   Ze maken landelijke vergelijkingen mogelijk — zonder betrouwbare data geen betrouwbare inzichten.
3. Ondersteunen van beleid en richtlijnontwikkeling  
   Door trends en uitkomsten te analyseren, kunnen registratiehouders bijdragen aan betere richtlijnen en standaarden.  
   Ze leveren bewijs voor wat werkt en wat niet, wat weer wordt gebruikt door beroepsgroepen, zorgaanbieders en overheid.
4. Zichtbaarheid en transparantie vergroten  
   Registratiehouders publiceren vaak geaggregeerde resultaten op platforms zoals Zorginzicht.nl of ZorgkaartNederland.nl.  
   Dit helpt burgers, patiënten en beleidsmakers om inzicht te krijgen in de prestaties van de zorg.
5. Verantwoording en toezicht faciliteren  
   Instanties zoals de IGJ, NZa en zorgverzekeraars gebruiken de gegevens uit kwaliteitsregistraties voor toezicht of inkoop.  
   Registratiehouders zijn dus een schakel tussen praktijk en beleid.

### **Verwerkingslocaties**

Benoem in welke landen de gegevensverwerkingen plaatsvinden. Beschrijf het doorgiftemechanisme dat van toepassing is wanneer verwerkingslocaties zich buiten de Europese Economische Ruimte bevinden en benoem of en welke aanvullende maatregelen van toepassing zijn.

*\* Tekstsuggestie \**

De dataoverdracht en analyses vinden plaats in de verwerkingsomgeving van Naam registratiehouder of diens verwerker.

Er is wel/géén sprake van doorgifte naar een land buiten de Europese Economische Ruimte (EER).

De verwerkingslocatie is *[bijv. naam verwerker en vestigingsplaatsen verwerkingslocaties verwerker]*.

### **Juridisch en beleidsmatig kader**

Benoem de wet- en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de gegevensverwerkingen.

*\* Tekstsuggestie \**

Naam registratiehouder mag op grond van artikel 11p lid 1 Wkkgz gegevens, waaronder persoonsgegevens, waaronder gegevens over gezondheid, genetische gegevens of persoonsgegevens waaruit ras of etnische afkomst blijken, verwerken, voor zover dit noodzakelijk is om de kwaliteit van zorg aan de cliëntenpopulatie waarop de Naam kwaliteitsregistratie ziet te meten en te verbeteren.

### **Bewaartermijnen**

Bepaal en motiveer de bewaartermijnen van de (gepseudonimiseerde) persoonsgegevens aan de hand van 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.

*\* Tekstsuggestie \**

Voor alle bestanden die Naam registratiehouder ontvangt en verwerkt is Naam registratiehouder verantwoordelijk voor verwijdering.

**Bewaartermijnen persoonsgegevens**

|  |  |  |  |
| --- | --- | --- | --- |
| Bestanden met (gepseudonimiseerde) persoonsgegevens | Ingang bewaartermijn | Termijn | Motivatie |
| Aanleverbestand zorgaanbieder | Vanaf het moment van ontvangst | X weken | Invullen door registratiehouder |
| BASIS-gegevensset | Vanaf het moment van aanmaken | X jaar | Invullen door registratiehouder |
| PLUS-gegevensset | Vanaf het moment van aanmaken | X jaar | Invullen door registratiehouder |
| Back-up bestanden |  | X tijd | Retentieperiode is standaard ingesteld op … |

**Beleid**

In het kader van de bewaartermijnen maakt Naam registratiehouder onderscheid tussen gepseudonimiseerde persoonsgegevens in de aanleverbestanden en in de registratiebestanden (de BASIS- en de PLUS-gegevensset).

## Beoordeling rechtmatigheid gegevensverwerking

Beoordeel aan de hand van de feiten zoals vastgesteld in onderdeel A of de voorgenomen gegevensverwerkingen rechtmatig zijn. Het gaat hier om de beoordeling van de juridische rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen. Beoordeel tevens de wijze waarop invulling wordt gegeven aan de rechten van de betrokkenen.

Voor dit onderdeel van de DPIA is in het bijzonder juridische expertise nodig.

### **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.

Het enkel hebben van een wettelijke grondslag is voor de verwerking van (bijzondere) persoonsgegevens niet voldoende. Er dient ook aan andere bepalingen uit de AVG te worden voldaan.



*\* Tekstsuggestie \**

Naam registratiehouder mag ingevolge artikel 6 lid 1 sub e AVG jo. artikel 6 lid 3 sub b AVG jo. artikel 11p Wkkgz, bijzondere persoonsgegevens verwerken om haar taak van algemeen belang te vervullen. De ‘taak van algemeen belang’ die aan Naam registratiehouder is opgedragen, is het meten en verbeteren van de kwaliteit van zorg van de cliëntenpopulatie waarop de Naam kwaliteitsregistratie betrekking heeft.

### **Bijzondere persoonsgegevens**

Het verwerken van bijzondere persoonsgegevens is in beginsel verboden. Verwerking is pas mogelijk wanneer een uitzonderingsgrond van toepassing is. Beoordeel of een van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van het (gepseudonimiseerd) BSN: beoordeel of dit is toegestaan.

Vergelijk ook overwegingen 52, 53 en 54 bij de AVG, waarin uitdrukkelijk het belang wordt erkend van verwerkingen van bijzondere persoonsgegevens om redenen van algemeen belang op het gebied van volksgezondheid, het beheer van gezondheidszorgdiensten en -stelsels, met het oog op (onder meer) kwaliteitscontrole.



*\* Tekstsuggestie \**

Naam registratiehouder verwerkt ten behoeve van het meten en verbeteren van kwaliteit van zorg bijzondere persoonsgegevens als bedoeld in artikel 9 AVG. De grondslag voor verwerking van deze bijzondere persoonsgegevens betreft artikel 9 lid 2 sub i AVG jo. artikel 11p Wkkgz.

**Waarborgen**

Artikel 9 lid 2 sub i AVG vereist dat er “passende en specifieke maatregelen zijn genomen ter bescherming van de rechten en vrijheden van de betrokkene, met name het beroepsgeheim”.

Er zijn strikte technische en organisatorische maatregelen genomen om de beveiliging van de datasets zo goed mogelijk te borgen. Er wordt bij Naam registratiehouder en/of haar verwerker(s) gebruikgemaakt van goed beveiligde dataplatforms/remote access omgevingen/secure processing environments om de analyses uit te voeren. Naam registratiehouder ontvangt en verwerkt uitsluitend aan de bron gepseudonimiseerde gegevens die door Naam registratiehouder niet te herleiden zijn naar een individuele patiënt. Naam registratiehouder verbiedt personen die werkzaamheden verrichten voor Naam registratiehouder of voor een onder diens verantwoordelijkheid werkzame verwerker om pseudonimisering van persoonsgegevens ongedaan te maken. Onder het ongedaan maken van pseudonimisering wordt verstaan: het actief herleiden van gepseudonimiseerde gegevens naar natuurlijke personen, direct of indirect, door het combineren van gegevens of het gebruik van aanvullende informatie.

Dit verbod is van toepassing op:

* Het gebruik van technische middelen of databronnen om identificerende gegevens terug te halen;
* Het opvragen of benaderen van sleutelbestanden of koppelvariabelen zonder autorisatie;
* Het combineren van gepseudonimiseerde gegevens met andere datasets met als doel re-identificatie.

Overtreding van deze bepaling wordt door Naam registratiehouder aangemerkt als een ernstige schending van het gegevensbeschermingsbeleid en kan leiden tot disciplinaire maatregelen, waaronder beëindiging van het dienstverband.

Naam registratiehouder verbiedt (conform artikel 11p lid 3 Wkkgz) personen die werkzaamheden verrichten voor de Naam registratiehouder of een onder diens verantwoordelijkheid werkzame verwerker om hetgeen hen uit of in verband met die werkzaamheden over natuurlijke personen blijkt of wordt meegedeeld, verder bekend te maken dan voor het functioneren van de kwaliteitsregistratie noodzakelijk is dan wel op grond van de Wkkgz is voorgeschreven of toegestaan.

Naam registratiehouder voldoet aan de toetsingscriteria die opgesteld zijn door de Inhouds-governancecommissie (IGC) en de Data-governancecommissie (DGC). Deze toetsingscriteria toetsen o.a. het voldoen aan wet- en regelgeving (compliance). Een belangrijk onderdeel is de toetsing van de inrichting van de gegevensbescherming.

De inrichting van de gegevensbescherming is in lijn met de NEN7510/NEN7512 en/of ISO27001. Naam registratiehouder kan middels een in control statement en een verklaring van toepasselijkheid aantonen dat de genomen technische en organisatorische maatregelen passend zijn om een op het risico afgestemd beveiligingsniveau te waarborgen.

Of:

De inrichting van de gegevensbescherming wordt periodiek extern ge-audit en gecertificeerd conform de NEN7510 en/of ISO27001 of middels een SOC2 verklaring. Naam registratiehouder kan daarmee aantonen dat de genomen technische en organisatorische maatregelen passend zijn om een op het risico afgestemd beveiligingsniveau te waarborgen.

### **Doelbinding**

Indien de (gepseudonimiseerde) 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.

De wettelijke grondslag voor kwaliteitsregistraties gecreëerd in de Wkkgz geldt uitsluitend ten behoeve van de doelen leren en verbeteren en samen beslissen.



Het is uitdrukkelijk niet de bedoeling dat de registratiehouder gegevens verzamelt met als primair doel het uitvoeren van wetenschappelijk onderzoek. Tevens is het de registratiehouder (als verwerkingsverantwoordelijke) niet toegestaan om de (gepseudonimiseerde) persoonsgegevens aan derden te verstrekken voor het doen van wetenschappelijk onderzoek.



*\* Tekstsuggestie \**

Naam registratiehouder mag op grond van artikel 11p lid 1 Wkkgz gegevens, waaronder persoonsgegevens, waaronder gegevens over gezondheid, genetische gegevens of persoonsgegevens waaruit ras of etnische afkomst blijken, verwerken, voor zover dit noodzakelijk is om de kwaliteit van zorg aan de cliëntenpopulatie waarop de betreffende kwaliteitsregistratie ziet te meten en te verbeteren. Verder bepaalt artikel 11p lid 1 Wkkgz dat de verwerking alleen plaatsvindt indien:

1. dit noodzakelijk is op grond van het bij de aanvraag als bedoeld in artikel 11o, eerste lid, onderdeel f, onder 1°, omschreven doel van die kwaliteitsregistratie;
2. deze beperkt is tot de daarbij omschreven gegevens, verwerkingshandelingen, bewaartermijnen en cliëntenpopulatie; en
3. de gegevens afkomstig zijn van een zorgaanbieder die valt onder een daarbij omschreven categorie van zorgaanbieders.

[Optioneel] Naam registratiehouderis van mening dat hij als verwerkingsverantwoordelijke de ontvangen gegevens óók verder mag verwerken voor wetenschappelijk onderzoek en statistiek, voor dóórontwikkeling van de kwaliteitsregistratie en/of onderhoud en beheer van de dataset. Om de gegevens voor wetenschappelijk onderzoek en statistiek te mogen gebruiken, verwijst registratiehouder naar artikel 5 lid 1 sub b AVG, dat eist dat passende waarborgen worden getroffen voor de rechten en vrijheden van de betrokkene, waaronder minimale gegevensverwerking en pseudonimisering. Elders in deze DPIA zijn deze waarborgen beschreven.

### **Noodzaak en evenredigheid**

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

1. Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden (ervan uitgaande dat met de verwerking van gegevens het doel bereikt kan worden)?
2. Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt?

De beginselen noodzakelijkheid, proportionaliteit en subsidiariteit komen zowel in de AVG als in de Wkkgz en bijbehorende ministeriële regeling voor. Toch verschilt de toepassing en het bereik van de beginselen in de twee wetten. In de AVG zijn de beginselen privacy gerelateerd: is een verwerking noodzakelijk voor het genoemde doel en is de inbreuk op de persoonlijke levenssfeer proportioneel en subsidiair; waarbij de termen uitgelegd kunnen worden zoals hierboven (onder kop 14) beschreven. In de Wkkgz en de bijbehorende ministeriële regeling zijn deze termen niet enkel privacy gerelateerd, maar gaan deze verder dan dat.[[4]](#footnote-5)



Een kwaliteitsregistratie dient aan zowel de eisen van de AVG als de Wkkgz en bijbehorende ministeriële regeling te voldoen. In dit onderdeel van de DPIA beschrijft de registratiehouder echter enkel waarom de kwaliteitsregistratie noodzakelijk, proportioneel en subsidiair is, zoals bedoeld in de AVG.

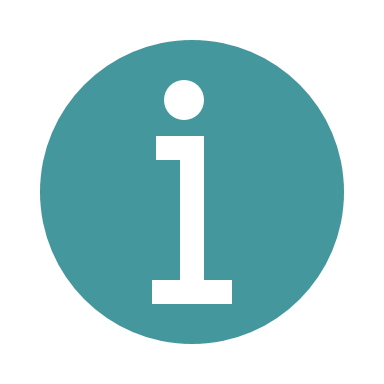
*\* Tekstsuggestie \**

De Naam kwaliteitsregistratie voldoet aan de beginselen van noodzakelijkheid, proportionaliteit en subsidiariteit (zoals bedoeld in de AVG), omdat aanvullen.

Naam registratiehouder heeft in bijgevoegde verantwoordingstabel onderbouwd welke (gepseudonimiseerde) persoonsgegevens noodzakelijk zijn voor de doelen van de kwaliteitsregistratie.

### **Rechten van betrokkenen**

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

 Het geval van registratiehouders als verwerkingsverantwoordelijken is een bijzondere situatie. Dit komt doordat registratiehouders enkel beschikken over gepseudonimiseerde gegevens van de zorgaanbieders. Zij beschikken daarbij niet over de sleutel van die pseudoniemen. Registratiehouders kunnen hierdoor de gepseudonimiseerde gegevens niet de-pseudonimiseren en de patiënten in hun kwaliteitsregistratie niet herkennen. De situatie van artikel 11 lid 2 AVG doet zich in die gevallen voor, waardoor de artikel 15 t/m 20 AVG (en de daarin beschreven rechten van betrokkenen) niet van toepassing zijn. Dit is anders wanneer de betrokkene extra gegevens aan de registratiehouder verstrekt (zoals bijvoorbeeld zijn pseudoniemsleutel), waardoor de patiënt/betrokkene wel herkenbaar wordt in de kwaliteitsregistratie voor de registratiehouder.

*\* Tekstsuggestie \**

**Recht op informatie (art. 13 en 14 AVG)**

Op de website van Naam registratiehouder is een privacyverklaring te vinden: url.

**Recht op inzage (art. 15 AVG)**

In beginsel is dit recht niet van toepassing, tenzij de patiënt/betrokkene zich meldt met aanvullende gegevens en de patiënt/betrokkene wel te identificeren is. In dat geval aanvullen.

**Recht op rectificatie of aanvulling van gegevens (art. 16 AVG)**

In beginsel is dit recht niet van toepassing, tenzij de patiënt/betrokkene zich meldt met aanvullende gegevens en de patiënt/betrokkene wel te identificeren is. In dat geval aanvullen.

**Recht op vergetelheid (art. 17 AVG)**

In beginsel is dit recht niet van toepassing, tenzij de patiënt/betrokkene zich meldt met aanvullende gegevens en de patiënt/betrokkene wel te identificeren is. In dat geval aanvullen.

**Recht op beperking van de verwerking (art. 18 AVG)**

In beginsel is dit recht niet van toepassing, tenzij de patiënt/betrokkene zich meldt met aanvullende gegevens en de patiënt/betrokkene wel te identificeren is. In dat geval aanvullen.

**Recht op gegevensoverdraagbaarheid (art. 20 AVG)**

In beginsel is dit recht niet van toepassing, tenzij de patiënt/betrokkene zich meldt met aanvullende gegevens en de patiënt/betrokkene wel te identificeren is. In dat geval aanvullen.

**Recht op bezwaar (art. 21 AVG)**

In beginsel kan er géén uitvoering worden gegeven aan het recht van bezwaar, omdat de registratiehouder de patiënt/betrokkene niet kunnen identificeren in de dataset. Dit is anders wanneer de patiënt/betrokkene extra gegevens aan de registratiehouder verstrekt, waardoor de patiënt/betrokkene wel te identificeren is in de dataset. In dat geval aanvullen.

**Recht om niet te worden onderworpen aan geautomatiseerde besluitvorming (art. 22 AVG)**

Bij de Naam kwaliteitsregistratie wordt er geen geautomatiseerde besluitvorming toegepast.

## 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 gegevensverwerking zoals in onderdeel A en B zijn beschreven en beoordeeld. Het gaat hierbij overigens niet om de risico’s van de verwerkingsverantwoordelijke (registratiehouder) zelf.

### **Risico’s voor betrokkenen**

Beschrijf en beoordeel de risico’s van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Maak hierbij een risico-inschatting op basis van kans x impact:

|  |  |  |  |
| --- | --- | --- | --- |
| Kans | | Impact | |
| Hoog | Zeer waarschijnlijk | Hoog | Forse impact op betrokkene |
| Medium | Denkbaar | Medium | Beperkte impact op betrokkene |
| Laag | Onwaarschijnlijk | Laag | Weinig of verwaarloosbare impact op de betrokkene |

Ter ondersteuning vindt u hieronder voorbeelden van risico’s.[[5]](#footnote-6) De kolom met mogelijke maatregelen kunt u gebruiken voor onderdeel D (punt 17).

|  |  |  |
| --- | --- | --- |
| Thema | Voorbeelden van risico’s | Mogelijke maatregelen |
| Rechtmatige en transparante verwerking | * Verwerken zonder rechtsgrond * Onvoldoende informatie aan betrokkenen | * Verwerkingsgrondslagen vastleggen * Heldere privacyverklaring en communicatie |
| Beperking van doelbinding | * Gegevens gebruiken voor andere doeleinden dan waarvoor verzameld | * Doelbinding vastleggen en toezien op beperking * Bewaken van doelwijzigingen |
| Minimalisatie van persoonsgegevens | * Verzamelen van onnodige gegevens * Onnodig bewaren | * Alleen noodzakelijke gegevens verzamelen * Dataminimalisatie en -opschoning |
| Beveiliging van persoonsgegevens | * Onvoldoende technische en organisatorische maatregelen (bijv. encryptie, toegangsbeheer) | * Encryptie, 2FA, toegangscontroles * Beveiligingsbeleid en bewustwording |
| Rechten van betrokkenen waarborgen | * Geen of onvolledige procedures voor verzoeken van betrokkenen | * Procedures voor inzage, correctie, verwijdering * Training van medewerkers |
| Governance en accountability | * Geen privacybeleid * Onduidelijke verantwoordelijkheden | * Privacybeleid opstellen en koppelen aan procedures en werkinstructies * Privacyfunctionarissen aanstellen * Documentatie bijhouden |
| Toezicht op ontvangers (waaronder (sub)verwerkers) | * Onvoldoende contractuele afspraken of toezicht op ontvangers/verwerkers | * Passende overeenkomsten * Due diligence en audits bij ontvangers/verwerkers |
| Specifieke bescherming van bijzondere persoonsgegevens | * Onvoldoende bescherming van gezondheidsgegevens, biometrische of andere bijzondere persoonsgegevens | * Specifieke aanvullende, passende technische maatregelen * DPIA’s uitvoeren op grootschalige verwerkingen van bijzondere persoonsgegevens |
| Bewaartermijnen en gegevensopslag | * Onnodig lang bewaren van gegevens | * Bewaartermijnen vaststellen en handhaven * Periodieke data-opruiming |
| Detectie en melding van datalekken | * Onbedoelde openbaarmaking, onrechtmatige toegang, verlies van gegevens | * Datalekkenbeleid en meldprocedures * Training van personeel en bewustwording |

*\* Voorbeeld voor rapportage \**

|  |  |  |  |
| --- | --- | --- | --- |
| Beschrijving risico | Kans | Impact | Risico-inschatting |
| Ongeautoriseerde gebruiker krijgt toegang tot systeem met verzamelde persoonsgegevens. | Laag | Medium | Laag |
| Verzamelde gegevens worden niet na einde bewaartermijn verwijderd. | Medium | Medium | Medium |
| Gegevens gebruiken voor andere doeleinden dan waarvoor verzameld. | Medium | Hoog | Hoog |
| Etc. |  |  |  |

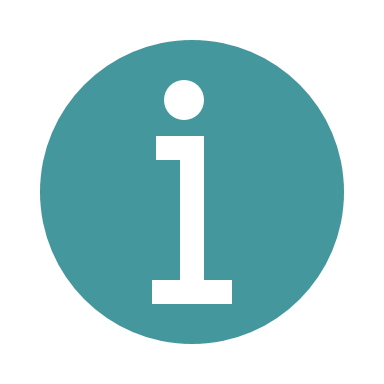
## Beschrijving voorgenomen maatregelen

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 verwerkingsverantwoordelijke (of wetgever).

Voor dit onderdeel van de DPIA is, als het gaat om beveiligingsmaatregelen, 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 en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.

 De tabel dient als volgt te worden ingevuld:

* Onder ‘risico’ wordt een beschrijving gegeven van een bestaand risico binnen de gegevensverwerkingen (zoals benoemd onder punt 16).
* Onder ‘maatregelen’ dienen alle maatregelen te worden genoemd die geïmplementeerd worden om het risico zoveel mogelijk te verminderen.
* De ‘beheerder van maatregelen’ is de persoon of het organisatieonderdeel die verantwoordelijk (niet verwerkingsverantwoordelijke) is voor het feit dat de maatregelen worden uitgevoerd.
* Onder ‘resterend risico en risico-inschatting’ dient te worden beschreven welke resterende risico’s overblijven na het nemen van de maatregelen. De kleur van het vlak geeft aan wat de risico-inschatting is voor het resterende risico. Deze risico-inschatting wordt weer uitgevoerd op basis van het principe kans x impact. Beschrijf het resterende risico in het vlak en geef met de kleuren groen (laag risico), geel (gemiddeld risico) en rood (hoog risico) aan wat de risico-inschatting is op basis van het principe kans x impact. Dit wordt niet uitdrukkelijk opgenomen in de tabel om de tabel overzichtelijk te houden.

*\* Voorbeeld voor rapportage \**

|  |  |  |  |
| --- | --- | --- | --- |
| Risico | Maatregelen | Resterend risico en risico-inschatting | Beheerder van maatregelen |
| Ongeautoriseerde gebruiker krijgt toegang tot systeem met verzamelde persoonsgegevens. | * Verzamelde persoonsgegevens in systeem zijn gepseudonimiseerd en sleutelgegevens zijn buiten het systeem opgeslagen. * Twee factor authenticatie geïmplementeerd voor inloggen in systeem. | Gebrek aan BYOD-beleid, zorgt ervoor dat het beveiligingssysteem niet weet wanneer een geautoriseerd apparaat of ongeautoriseerd apparaat toegang heeft. | Productmanager  Systeembeheerder |
| Verzamelde gegevens worden niet na einde bewaartermijn verwijderd. | Procedure geïmple­menteerd en verantwoor­delijke functionarissen aangewezen, zodat periodiek wordt gecontroleerd of bewaartermijn wordt gehonoreerd | Verantwoordelijke functionaris heeft geen toegang tot alle bronlocaties van alle gegevens om gegevens te verwijderen, waaronder automatische back-ups. | Productmanager  Systeembeheerder |
| Onrechtmatige verwerking van persoonsgegevens. | Trainingen en bewustwordings-programma’s voor medewerkers geïmplementeerd. | Grondslag gegevensverwerking wordt verkeerd geïnterpreteerd. | Jurist  Privacy officer |

## Conclusie en ondertekening

Beschrijf de conclusie van de uitgevoerde DPIA. Denk hierbij aan: Wordt de gegevensverwerking gestart/voortgezet of niet? Indien er instructies/adviezen zijn gegeven door de FG, vat deze hier samen. Ga in op eventuele resterende risico’s en vervolgstappen die worden genomen. Waar mogelijk, blik terug op de vorige uitgevoerde DPIA en de ontwikkelingen die zijn gemaakt.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Naam, functie** is tekenbevoegd en verklaart akkoord te zijn met de inhoud van deze DPIA.

**Datum ondertekening:**

**Handtekening:**

1. Guidelines on Data Protection Impact Assessment (DPIA), wp248rev.01. [↑](#footnote-ref-2)
2. Waar in deze DPIA sprake is van persoonsgegevens worden daar te allen tijde door de verstrekker (aan de bron) gepseudonimiseerde persoonsgegevens mee bedoeld. [↑](#footnote-ref-3)
3. Na inwerkingtreding van de op-out verplichting (één jaar na inwerkingtreding van de Wkz) geldt ook:

   *… en die bij de zorgaanbieder niet aangegeven hebben bezwaar te hebben (opt-out) tegen de verstrekking van zijn/haar gegevens aan registratiehouder. Wanneer een zorgaanbieder een bezwaar tegen verstrekking (opt-out) ontvangt, worden bij een volgende aanlevering van zorgaanbieder de gegevens van de betreffende betrokkene uit de dataset gehaald.* [↑](#footnote-ref-4)
4. Zie artikel 7ab van de ministeriële regeling, inclusief bijbehorende uitleg. [↑](#footnote-ref-5)
5. Bron: NOREA Privacy Control Framework [↑](#footnote-ref-6)