



Data Protection Impact Assessment (DPIA)

Verwerking diagnosegegevens geestelijke gezondheidszorg door het CBS

CENTRAAL BUREAU VOOR DE STATISTIEK

DIRECTIE STRATEGIE EN BESTUURSADVISING

DEN HAAG 3 januari 2023



Vaststelling verwerkersverantwoordelijke: 5 januari 2023

Naam: Mw. A. Berg

Advies 5.1.2.e 5 januari 2023

Naam: 5.1.2.e

Advies CIO: 5 januari 2023

Naam: Dhr. W. van Nunspeet

Data Protection Impact Assessment (DPIA)

**Verwerking diagnosegegevens geestelijke gezondheidszorg
door het CBS**

DIRECTIE STRATEGIE EN BESTUURSADVISING

Contact:

Centraal bureau voor de statistiek

5.1.2.e

Email: 5.1.2.e [@cbs.nl](mailto:5.1.2.e@cbs.nl)

Telefoonnummer (5.1.2.e): (5.1.2.e)

Versie: 1.0 11 januari 2023

Inhoudsopgave

Inleiding	5
A. Beschrijving kenmerken gegevensverwerkingen	6
1. Voorstel 	6
2. Persoonsgegevens 	8
3. Gegevensverwerkingen 	9
4. Verwerkingsdoeleinden 	10
5. Betrokken partijen 	10
6. Belangen bij de gegevensverwerking 	12
7. Verwerkingslocaties 	12
8. Techniek en methode van gegevensverwerking 	13
9. Juridisch en beleidsmatig kader 	13
10. Bewaartermijnen 	14
B. Beoordeling rechtmatigheid gegevensverwerkingen	15
11. Rechtsgrond 	15
12. Bijzondere persoonsgegevens 	15
13. Doelbinding 	17
14. Noodzaak en evenredigheid 	17
15. Rechten van de betrokkene 	18
C. Beschrijving en beoordeling risico's voor de betrokkenen	19
16. Risico's 	19
D. Beschrijving voorgenomen maatregelen	19
17. Maatregelen 	19

Inleiding

Voorliggend document betreft de Data Protection Impact Assessment (DPIA) op het verzamelen en verwerken van diagnosegegevens uit de geestelijke gezondheidszorg (GGZ) door het CBS.

Per april 2017 is de Nederlandse Zorgautoriteit (NZa) gestopt met het verzamelen van gedetailleerde DSM-diagnoses¹ van volwassenen die behandeld worden in de gespecialiseerde GGZ. GGZ diagnoses op hoofdgroepenniveau werden tot 2022 nog wel verzameld binnen de DBC-financieringssystematiek, en in de eerste twee jaren van het nieuwe Zorgprestatiemodel. De uitvraag van diagnose-informatie komt vanaf 2024 te vervallen. Dit betekent dat vanaf verslagjaar 2024 er geen informatie over behandelde psychische problematiek in de GGZ meer beschikbaar is voor monitoring, onderzoek en statistiek. Het CBS heeft zich de afgelopen periode ingespannen om de continuïteit van de GGZ diagnosegegevens te borgen. In deze DPIA zijn de gegevensbeschermingsrisico's behorend bij de verzameling en verwerking van GGZ diagnosegegevens beschreven en zijn maatregelen benoemd om deze risico's te mitigeren.

De DPIA heeft de volgende opbouw:

- A. Beschrijving kenmerken van de gegevensverwerking
- B. Beoordeling van rechtmatigheid gegevensverwerking
- C. Beschrijving en beoordeling van de risico's voor de betrokkenen
- D. Beschrijving voorgenomen maatregelen

¹ DSM - Diagnostic and Statistical Manual of Mental Disorders, het standaard classificatiesysteem van psychische stoornissen.

A. 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 PIA: een overzicht van de relevante feiten van de voorgenomen gegevensverwerkingen. Als de feiten onduidelijk zijn, werkt dit door in de beoordeling.

1. Voorstel



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

Algemeen: Het CBS is een zelfstandig bestuursorgaan opgericht bij wet: de Wet op het Centraal bureau voor de statistiek (verder 'CBS-wet'). In het kader van de statistiek verwerkt het CBS als verantwoordelijke persoonsgegevens langs geautomatiseerde en handmatige weg.

Taak: Het CBS heeft tot taak het van overheidswege verrichten van statistisch onderzoek ten behoeve van praktijk, beleid en wetenschap en het openbaar maken van de resultaten van deze statistische onderzoeken (artikel 3 CBS-wet).

Uitvoeren (grondslag): Voor het uitvoeren van zijn taak verzamelt het CBS (artikel 33 CBS-wet i.c.m. artikel 6.1 (e) AVG) onder meer persoonsgegevens bij respondenten en bedrijven, waaronder zorgaanbieders. De GGZ diagnosegegevens worden gebruikt bij statistische analyses. De verzamelde gegevens worden niet langer bewaard dan noodzakelijk voor de statistische taken van het CBS en dus vernietigd zodra ze in dat kader niet meer nodig zijn.

Gebruik van de gegevens (doelbinding): De door de directeur-generaal van de statistiek (DG) in het kader van de uitoefening van de taken ter uitvoering van de CBS-wet ontvangen gegevens mogen uitsluitend worden gebruikt voor statistische en wetenschappelijke doeleinden. Gebruik van de gegevens voor fiscale, administratieve, controle en gerechtelijke doeleinden is niet toegestaan (zie de memorie van toelichting bij artikel 37 lid 1 CBS-wet). De GGZ diagnosegegevens worden opgevraagd bij zorgaanbieders en gecombineerd met informatie uit het Zorgprestatie-model voor de continuering van langer lopende statistieken over behandelde problematiek in de geestelijke gezondheidszorg die voorheen waren gebaseerd op informatie uit de DBC's GGZ². In deze statistieken wordt de behandelde problematiek beschreven naar achtergrondkenmerken van de behandelde personen, zoals leeftijd, geslacht, inkomensgroep, herkomst en regio. Ook worden de gegevens gecombineerd met kenmerken van de geboden zorg, zoals het type aanbieder en setting. Tot 2016 was gedetailleerde diagnoseinformatie beschikbaar, het is de bedoeling vergelijkbare StatLine-tabellen opnieuw te kunnen publiceren.

In combinatie met andere bij het CBS beschikbare gegevens kunnen vragen beantwoord worden als:

- Wat is het perspectief op werk voor mensen die eerder voor depressie zijn behandeld?
- Hoeveel mensen in Nederland krijgen een behandeling voor een angststoornis en is dat meer of minder dan in andere Europese landen?
- Hoeveel mensen zijn behandeld voor een gokverslaving? En hoe vaak speelde er tegelijkertijd ook andere psychische problematiek?
- Wat zijn de landelijke zorguitgaven voor de behandeling van verschillende psychische problemen?
- Wat is de oversterfte van mensen met een diagnose schizofrenie of bipolaire stoornis ten opzichte van de algemene bevolking, en hoe verhoudt die zich tot andere Westerse landen (OECD-kwaliteitsindicator)?
- Werkt de gerichte aanpak van depressiepreventie voor risicogroepen (via het Meerjarenprogramma Depressiepreventie)?

Toegang tot de data: De toegang tot de GGZ diagnosegegevens is alleen mogelijk voor degenen die belast zijn met de uitvoering van de taak van het CBS en die in dat kader noodzakelijkerwijs toegang moeten hebben tot de betreffende data. Het CBS is het nationale statistische instituut en heeft beleid en procedures geïmplementeerd die waarborgen dat de gegevens uitsluitend voor wetenschappelijke en statistische doeleinden kunnen worden gebruikt. Deze waarborgen zijn zowel in internationale regelgeving (Verordening (EG) Nr. 223/2009

² [DBC-gefinancierde geestelijke gezondheidszorg \(GGZ\), hoofddiagnoses \(cbs.nl\)](#)

betreffende de Europese statistiek en de Praktijkcode voor Europese Statistieken) als in nationale regelgeving (CBS-wet) opgenomen. Ook de gedragscode CBS besteedt aandacht aan dit aspect.

Op verzoek kan de DG toegang verlenen tot een verzameling van gegevens of gegevens verstrekken ten behoeve van statistisch en wetenschappelijk onderzoek indien passende maatregelen zijn genomen om herkenning van afzonderlijke personen, huishoudens en ondernemingen te voorkomen (artikel 41 CBS-wet). Met behulp van remote access worden de gegevens door andere instellingen geanalyseerd en resultaten van het onderzoek worden op geaggregeerd niveau gepubliceerd.

Maatregelen zijn onder andere:

1. De DG kan (organisatieonderdelen van) instellingen alleen toegang verlenen tot analysebestanden indien zij uitsluitend tot doel en taak hebben het doen van wetenschappelijk onderzoek;
2. De DG kan alleen aanvragen tot microdata van een onderzoeker goedkeuren indien zij uitsluitend tot doel en taak hebben het doen van wetenschappelijk onderzoek.

Meer informatie over de Remote Access omgeving is te vinden op [de website van het CBS](#). Zie tevens einde punt 17 van deze PIA.

Geheimhouding: de verzamelde GGZ diagnosegegevens worden door het CBS nooit herleidbaar tot een identificeerbare persoon openbaar gemaakt. Publicatie is alleen in geaggregeerde vorm mogelijk (artikel 37 lid 3 CBS-wet). Het CBS voert hierop zogeheten outputcontroles uit. Werknemers van het CBS hebben als ambtenaar een eed of belofte afgelegd en zijn verplicht tot geheimhouding conform artikel 5 en 9 van de Ambtenarenwet. Onderzoekers van andere instellingen dienen te tekenen voor geheimhouding in een overeenkomst en geheimhoudingsverklaring.

Beveiliging: Het Burgerservicenummer (BSN) wordt tijdens het dataverzamelingsproces twee keer versleuteld (gepseudonimiseerd) door ZorgTTP. De eerste versleuteling vindt plaats bij de zorgaanbieder. Een tweede versleuteling vindt plaats bij ZorgTTP. Ten slotte worden de pseudoniemen geconverteerd naar pseudoniemen van het CBS-specifieke domein, die aan het CBS geleverd worden. Binnen het CBS worden deze ZorgTTP-pseudoniemen vervangen voor CBS_eigen pseudoniemen. De analyses worden alleen uitgevoerd op bestanden met deze CBS-eigen pseudoniemen. In deze bestanden zijn geen gegevens beschikbaar over namen, adressen of geboortedata.

Toetsing: Het CBS laat zich jaarlijks extern toetsen op de informatiebeveiliging (ISO 27001), kwaliteit (ISO 9001) en de privacybescherming (Privacy Control Framework van NOREA). De certificaten worden op de website van CBS gezet. <https://www.cbs.nl/nl-nl/over-ons/organisatie/privacy/iso-en-privacycertificering>

2. Persoonsgegevens



Som alle categorieën van persoonsgegevens op die worden verwerkt. Geef per categorie van persoonsgegevens tevens aan op wie die betrekking hebben. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder, strafrechtelijk en wettelijk identificerend.

Het CBS mag zowel bijzondere als niet-bijzondere persoonsgegevens ontvangen en verder verwerken ten behoeve van zijn statistische taken mits de vereisten op grond van de genoemde relevante wet- en regelgeving in acht worden genomen. Zie ook [Bronnen](#) van het CBS.

Burger Servicenummer (BSN): De DG kan het Burgerservicenummer opnemen in een registratie en daarvan gebruik maken ten behoeve van statistische doeleinden. Het BSN kan gebruikt worden in contacten met personen en instanties voor zover deze zelf gemachtigd zijn tot het gebruik van dat nummer in een registratie (artikel 34 CBS-wet).

Bijzondere gegevens:

Het CBS kan ten behoeve van statistische doeleinden op grond van artikel 35 CBS-wet bijzondere categorieën van persoonsgegevens (artikel 9 AVG jo. Paragraaf 3.1 Uitvoeringswet AVG) verwerken zoals ras, etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens, gezondheid, seksueel gedrag of seksuele gerichtheid. Op basis van artikel 9 tweede lid, aanhef en onderdeel j en artikel 24 van de Uitvoeringswet AVG mogen de gegevens verwerkt worden indien de verwerking noodzakelijk is met het oog op wetenschappelijk onderzoek of statistische doeleinden overeenkomstig artikel 89, eerste lid van de verordening en er is voldaan aan de overige voorwaarden van artikel 24 van de Uitvoeringswet AVG. Zie verder punt 12 van deze DPIA.

Categorieën persoonsgegevens:

Categorie gegevens	Detail niveau	Typering persoonsgegevens	Relevantie
BSN	Individueel niveau	Uniek persoonsnummer voor iedereen die ingeschreven staat in de Basisregistratie Personen (BRP)	Variabele waarmee de koppeling aan CBS registers tot stand komt. (maar alleen in gespseudonimiseerde vorm)
DSM5 diagnose classificatie	Individueel niveau	Bijzonder persoonsgegevens	Kernvariabelen die het behandelde probleem/ de behandelde problemen weergeven, conform de classificatie in de DSM5. Nodig voor statistisch onderzoek naar behandelde problematiek in de GGZ.
Zorgtraject code	Individueel niveau	Bijzonder persoonsgegevens	Variabele waarmee de koppeling gemaakt kan worden met andere variabelen uit het zorgprestatie model.
Startdatum zorgtraject	Individueel niveau	Bijzonder persoonsgegevens	Kernvariabele nodig voor afbakening zorgtrajecten
AGB-code zorgaanbieder	Individueel niveau	Bijzonder persoonsgegevens	Variabele waarmee de koppeling gemaakt kan worden met andere variabelen uit het zorgprestatie model.

3. Gegevensverwerkingen

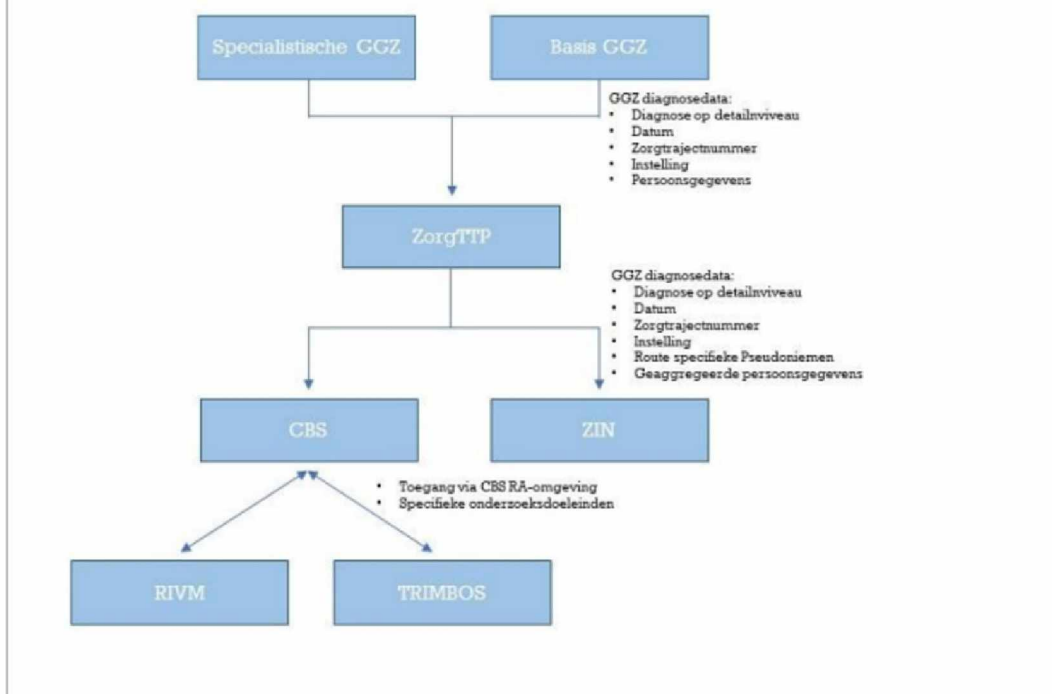


Geef alle voorgenoemen gegevensverwerkingen weer.

Zorgaanbieders in de specialistische en basis GGZ worden door het CBS benaderd om gegevens aan te leveren voor statistisch onderzoek. Door middel van een Privacy en Verzendmodule (PVM) kan de zorgaanbieder persoonsgegevens op een veilige manier versturen naar ZorgTTP. Na pseudonisatie in de PVM en een tweede maal bij ZorgTTP wordt de data beschikbaar gesteld aan het CBS.

Na ontvangst van de gepseudonimiseerde gegevens door het CBS volgt technische controle, koppelen, controle en correctie (editing), aggregeren en tabelleren, analyseren en publiceren, en tot slot bewaren (<https://www.cbs.nl/nl-nl/over-ons/organisatie/statistisch-proces>).

Fig 1 Schematische weergave verwerking persoonsgegevens



4. Verwerkingsdoeleinden



Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

Het CBS heeft tot taak het van overheidswege verrichten van statistisch onderzoek ten behoeve van praktijk, beleid en wetenschap en het openbaar maken van de resultaten van deze statistische onderzoeken (artikel 3 CBS-wet) en is verantwoordelijk voor het uitvoeren van statistische Europese verordeningen (artikel 4 CBS-wet).

Het verzamelen van GGZ diagnosegegevens stelt het CBS in staat om statistische informatie samen te stellen waarmee belangrijke vragen over ontwikkelingen in de GGZ beantwoord kunnen worden. De informatie helpt VWS en andere organisaties om beleid te onderbouwen en beleidsevaluaties uit te voeren. Ook draagt het bij aan onderzoek naar het verbeteren van de kwaliteit van de zorg en de effectiviteit en doelmatigheid van geleverde zorg. Daarnaast is het CBS verplicht (EU-verplichting) om op geaggregeerd niveau statistische uitkomsten te leveren aan Eurostat.

5. Betrokken partijen



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

Het CBS voldoet aan de hoogste eisen m.b.t. gegevensbescherming. De privacybescherming wordt jaarlijks getoetst in een Raamwerk Privacy Audit. Privacybescherming omvat het geheel van maatregelen dat een adequate bescherming van persoons- en bedrijfsgegevens waarborgt. Een groot deel van deze maatregelen heeft betrekking op de beveiliging van de gegevens en heeft daarmee overlap met de eisen voor informatiebeveiliging. In privacy audits komen dan ook aspecten van informatiebeveiliging aan de orde volgens het NOREA-kader. NOREA is de beroepsorganisatie van IT-Auditors (zie voor meer informatie over informatiebeveiliging punt 17 over maatregelen). Sinds 2015 worden er bij het CBS privacy audits gehouden. Deze worden uitgevoerd door een externe auditor en resulteert in een privacy-proof verklaring.

Tezamen met de certificering voor de ISO27001 is daarmee aan de wettelijke verantwoordingsplicht van de gegevensleverancier voldaan. Dit betekent ook dat zodra de bestanden door het CBS zijn ontvangen, de verantwoordelijkheid van de gegevensleverancier ophoudt. Het CBS is de verwerkingsverantwoordelijke. Daarnaast worden in een aantal gevallen bepaalde taken van het CBS uitbesteed aan derden (zogenaamde verwerkers). In het geval van de GGZ diagnosegegevens besteedt het CBS de verzameling van gegevens uit aan ZorgTTP.

CBS is verwerkersverantwoordelijke

Het CBS heeft op grond van artikel 3 CBS-wet de taak om statistieken te maken ten behoeve van beleid, praktijk en wetenschap. Conform artikel 18 CBS-wet bepaalt de DG CBS daarnaast de methoden waarmee de statistische onderzoeken worden uitgevoerd en de wijze waarop de resultaten van die onderzoeken openbaar worden gemaakt. Het CBS is daarin onafhankelijk en kan en mag hierin geen instructies van anderen aannemen. Verwerkingsverantwoordelijke (artikel 4 lid 7 AVG) is: de instantie die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Op grond van deze twee wettelijke bepalingen is het CBS altijd verwerkingsverantwoordelijke en nimmer verwerker.

Verwerkers

Het CBS besteedt het technische deel rondom het verzamelen van GGZ diagnosegegevens uit aan ZorgTTP. Het CBS heeft met ZorgTTP een verwerkersovereenkomst gesloten, waarin afspraken zijn gemaakt over de verwerking van de persoonsgegevens conform de AVG en de Uitvoeringswet, en, voor zover van toepassing en relevant, de Wet op het Centraal bureau voor de statistiek en andere wet- en regelgeving.

Verstrekker

Zorgaanbieders in de specialistische en basis GGZ beschikken over diagnosegegevens. Met een beroep op artikel 33 lid 1 aanhef onder a sub 1 en artikel 33 lid 4 van de Wet op het CBS verzoekt het CBS de zorgaanbieders om verstrekking van de benodigde diagnosegegevens.

Ontvangers

Gegevens kunnen passend beschermd (zie verder punt 17 van deze DPIA) en op verzoek worden verstrekt aan de volgende partijen conform CBS-wet:

- 1) medewerkers van het CBS belast met de uitvoering van de wettelijke taak van het CBS (artikel 37 lid 2);
- 2) ten behoeve van statistisch of wetenschappelijk onderzoek verstrekken aan een dienst, organisatie of instelling. Dit kunnen zijn (artikel 41):
 - a. een universiteit in de zin van de Wet op het hoger onderwijs en wetenschappelijk onderzoek;
 - b. een bij wet ingestelde organisatie of instelling voor wetenschappelijk onderzoek;
 - c. bij of krachtens de wet ingestelde planbureaus;
 - d. de communautaire en nationale instanties voor de statistiek van de lidstaten van de Europese Unie;

- e. onderzoeksafdelingen van ministeries en andere diensten, organisaties en instellingen.

6. Belangen bij de gegevensverwerking



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

Verwerkingsverantwoordelijke

De voorgenomen verwerking van GGZ diagnosegegevens is noodzakelijk om de taken van het CBS, het maken van statistieken ten behoeve van beleid, praktijk en wetenschap, te kunnen uitvoeren. Het niet verzamelen en verwerken van GGZ diagnosegegevens zou ertoe leiden dat relevante informatie over ontwikkelingen in de behandelde psychische problematiek ontbreekt. Dit heeft uiteenlopende gevolgen voor beleidsontwikkeling en monitoring en wetenschappelijk onderzoek naar GGZ zorg.

Verwerker

ZorgTTP heeft geen inhoudelijk belang bij het verzamelen en verwerken van de GGZ diagnosegegevens.

Verstrekker

De belangen van de verstrekkers (zorgaanbieders) richten zich met name op het borgen van de privacy van personen die geestelijke gezondheidszorg ontvangen. Het verstrekken van data aan derden leidt tot een verhoogd risico op datalekken, waardoor de kans op onthulling toeneemt.

Ontvanger

De voorgenomen verwerking van GGZ diagnosegegevens door het CBS is voor diverse partijen belangrijk:

- Onderzoeksinstituten waaronder het RIVM en TRIMBOS zijn voor de uitvoering van diverse onderzoeken op het gebied van de GGZ afhankelijk van de GGZ diagnosegegevens;
- Voor VWS en andere partijen zijn diagnosegegevens van belang voor het ontwikkelen en monitoren van beleid binnen de GGZ bijvoorbeeld om de effectiviteit en doelmatigheid van de GGZ te verbeteren.

7. Verwerkingslocaties



Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

Verwerkingslocaties zijn ZorgTTP (Houten) en CBS in Nederland (Den Haag, Heerlen). Het computercentrum van het CBS is gevestigd in Almere.

8. Techniek en methode van gegevensverwerking



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

Het CBS verwerkt alleen gegevens voor wetenschappelijk onderzoek of statistische doeleinden. Er is geen sprake van (semi-)geautomatiseerde besluitvorming of profilering.

Bij publicatie zijn de gegevens nooit te herleiden naar één persoon of een zeer homogene groep van personen (bijv. 'vrijwel alle mensen in deze wijk zitten onder de armoedegrens').

Tot voorjaar 2022 maakten zorgaanbieders in de GGZ gebruik van de privacy- en verzendmodule (PVM) van ZorgTTP om data aan te bieden aan de NZa. In de nieuwe beoogde situatie maken de zorgaanbieders nog steeds gebruik van een PVM om data te leveren. Deze zal door ZorgTTP geconfigureerd en getest worden en kan dan vervolgens beschikbaar worden gemaakt voor de zorgaanbieders. Met behulp van deze nieuw te configureren PVM zijn zorgaanbieders in staat om veilig GGZ-diagnosedata te versturen naar ZorgTTP.

Om data vervolgens te kunnen ontvangen van ZorgTTP wordt gebruik gemaakt van een Doel en Retour Module (DRM). Deze module stelt CBS in staat om de gepseudonimiseerde bestanden te kunnen ontvangen/downloaden.

Bij het verzenden van data door de zorgaanbieders met behulp van de PVM worden de identificeerbare persoonsgegevens bij de bron voor een eerste maal gepseudonimiseerd. Daarna wordt het bestand doorgestuurd naar het CMT van ZorgTTP, waar er een tweede pseudonimisatie plaatsvindt. Deze tweede pseudonimisatieslag wordt voor elke gegevensverzameling over een ander domein/route uitgevoerd. Dit betekent dat er voor elk gegevensverzameling unieke (domein specifieke) pseudoniemen worden gegenereerd voor de ontvanger. Met deze maatregel wordt voorkomen dat er ongeautoriseerde (indirecte) herleiding plaatsvindt door deze gepseudonimiseerde gegevens te verrijken met andere gepseudonimiseerde gegevens afkomstig van andere partijen. Slechts met behulp van ZorgTTP kan een geautoriseerde koppeling van gepseudonimiseerde gegevens van verschillende gegevensverzamelingen plaatsvinden. Pseudoniemen van een bepaalde gegevensverzameling kunnen dan 'vertaald' worden naar de pseudoniemen van een andere verzameling. Dit proces wordt ook wel domeinconversie genoemd. Het CBS maakt voor andere verzamelingen reeds gebruik van de pseudonimisatiedienst van ZorgTTP. Hierdoor beschikken zij reeds over eigen (domein specifieke) pseudoniemen.

Na ontvangst van de data door het CBS worden in de CBS-koppelomgeving de domein specifieke pseudoniemen vervangen voor de interne CBS pseudoniemen (RINPERSOON) en worden de diagnosegegevens met behulp van het volgnummer van ZorgTTP samengevoegd met de pseudoniemen. Vervolgens worden de gegevens beschikbaar gesteld voor statistisch en wetenschappelijk onderzoek.

Daarbij worden op hoofdlijnen de volgende beveiligingsmaatregelen benoemd: afscherming van productiegegevens van internet en scanning van alle gegevens van en naar productieomgeving; beveiligde werkstations; afscherming van gebruik gegevensdragers; toegangscontrole en beveiliging van gebouwen; pseudonimiseren van identificerende gegevens; toetsing van beveiligingsmaatregelen middels interne en externe audits en tests. Zie verder punt 17 van deze DPIA.

9. 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.

Het juridisch kader voor de uitvraag van GGZ-diagnosegegevens door het CBS vormen:

- de wet op het Centraal Bureau voor de statistiek
- de Statistical Law (Europese verordening 223/2009)
- de Europese gedragscode voor statistiek
- de CBS-gedragscode.

Het CBS mag gegevens ontvangen op grond van artikel 33 CBS-wet. Lid 4 van dit artikel bepaalt: *"De in het eerste lid bedoelde instellingen, diensten, lichamen en zelfstandige bestuursorganen, de in het tweede lid bedoelde rechtspersonen en de in het derde lid bedoelde ondernemingen, vrije beroepsbeoefenaren, instellingen en rechtspersonen verstrekken de in die leden bedoelde gegevens kosteloos op verzoek van de directeur-generaal binnen een bij algemene maatregel van bestuur te bepalen termijn. Daarbij kan geen beroep worden gedaan op geheimhoudingsverplichtingen, tenzij deze verplichtingen gebaseerd zijn op internationale regelgeving."*

10. Bewaartermijnen



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

In het kader van de bewaartermijnen maakt CBS een onderscheid tussen persoonsgegevens in de zogenaamde 'inputbase', 'microbase', en persoonsgegevens in 'tussenbestanden'.

Inputbase

De inputbase bevat de (versleutelde) persoonsgegevens zoals CBS die ontvangt. In dit geval zijn dit binnenkomende (ruwe) bestanden met GGZ diagnosegegevens. De pseudoniemen die door ZorgTTP zijn gegenereerd worden zo snel mogelijk na binnenkomst vervangen door CBS pseudoniemen.

GGZ diagnosegegevens worden door het CBS gebruikt voor jaarstatistieken. Hiervoor geldt een maximale bewaartermijn van 2,5 jaar na afloop van het verslagjaar waarop de data betrekking hebben.

Op deze wijze kan het CBS in noodzakelijke gevallen "terug naar de bron". Er is geen reden om deze bestanden langer te bewaren dan hierboven genoemd, omdat de gegevens die gebruikt worden voor het maken van statistieken bewaard worden in de microbase.

Microbase

De microbase bevat de gepseudonimiseerde bestanden uit de inputbase nadat deze verder zijn verwerkt en gereed gemaakt voor het maken van statistieken. De bestanden in de microbase liggen direct ten grondslag aan het statistische proces.

Persoonsgegevens in de microbase kunnen langdurig worden bewaard, waarbij elke 3 jaar wordt getoetst of de motivering voor het bewaren nog geldt. De niet-persoonsgegevens in de microbase worden permanent bewaard.

De voornaamste redenen voor (langer) bewaren van gegevens zijn de volgende:

- In geval van wijzigingen in bron, methode of proces is het vaak wenselijk om breuken die daardoor in tijdreeksen ontstaan, te herstellen. Dat kan het beste door microdata die in het verleden zijn gebruikt opnieuw te verwerken. Dit vormt veelal een reden om bestanden te bewaren.
- Voor longitudinaal onderzoek is het regelmatig nodig oude gegevens opnieuw te aggregeren om tabellen te maken die vergelijkbaar zijn met nieuw opgezette tabellen.
- De microdata in de microbase worden onder meer beschikbaar gesteld aan wetenschappers. De wettelijke kaders daarvoor zijn vastgelegd in de artikelen 39 tot en

met 42 van de CBS-wet. Vooraf kan niet worden voorspeld wat de vraag van deze wetenschappers is, waardoor het ondoenlijk is voor dit gebruik relevante aggregaten samen te stellen. Het feit dat er uit microgegevens geput kan worden en er over (steeds) langere perioden gegevens beschikbaar zijn, maakt deze voorziening juist relevanter. Overigens geldt dit ook voor (her-) gebruik van microgegevens door het CBS zelf. Bij data gebruikt voor promotieonderzoek geldt een bewaartermijn van 10 jaar.

Tussenbestanden

In het kader van het statistische verwerkingsproces worden op basis van microbase bestanden doorgaans verschillende 'tussenbestanden' gemaakt.

Tussenbestanden worden zolang bewaard als voor het lopend proces nodig. Dit betekent dat zij na afronding van een statistisch onderzoek worden verwijderd.

Tot slot geldt dat de bewaartermijn voor back-up bestanden drie weken is. Deze termijn is vermeld in de nota "Herziening Back-up-beleid" van 30 maart 2011.

B. Beoordeling rechtmatigheid gegevensverwerkingen

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 PIA is in het bijzonder juridische expertise nodig.

11. Rechtsgrond



Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.

De wettelijke taak en wettelijke verplichtingen vormen de rechtsgrond voor de verwerkingen van GGZ diagnosegegevens zoals deze zijn opgenomen in de CBS-wet (art. 3, 4 en 5 CBS-wet).

Op grond van artikel 41 CBS-wet is de directeur-generaal van de statistiek bevoegd ten behoeve van statistisch of wetenschappelijk onderzoek onderzoekers toegang te geven tot een verzameling van gegevens, waarbij het CBS de wettelijke verplichting heeft om maatregelen te nemen om herkenning van afzonderlijke personen, huishoudens, ondernemingen of instellingen te voorkomen. Op grond van artikel 42 CBS-wet willicht de directeur-generaal een verzoek om toegang op grond van artikel 41 CBS-wet slechts in, indien de verzoeker naar het oordeel van de directeur-generaal voldoende maatregelen heeft getroffen om te voorkomen dat de verzameling van gegevens voor andere doeleinden dan statistisch of wetenschappelijk onderzoek wordt gebruikt.

12. Bijzondere persoonsgegevens



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

Het CBS verwerkt, ten behoeve van statistische doeleinden bijzondere persoonsgegevens als bedoeld in artikel 9 AVG. De grondslag voor verwerking van deze bijzondere persoonsgegevens betreft artikel 9 lid 1 sub j AVG jo. artikel 89 AVG in combinatie met artikel 35 CBS-wet. Artikel 35 CBS-wet is in lijn met artikel 24 Uitvoeringswet AVG. Hierin wordt aangegeven dat het verbod om persoonsgegevens als bedoeld in artikel 9, te verwerken ten behoeve van wetenschappelijk onderzoek of statistiek niet van toepassing is voor zover:

- de verwerking noodzakelijk is met het oog op wetenschappelijk het onderzoek of historisch onderzoek of statistische doeleinden overeenkomstig artikel 89 eerste lid AVG;
- het onderzoek bedoeld onder punt 1 een algemeen belang dient;
- het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning kost; en
- de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkenen niet onevenredig wordt geschaad.

Het CBS verwerkt verder, eveneens ten behoeve van statistische doeleinden, persoonsgegevens als bedoeld in artikel 10 AVG. Gegevens inzake strafrechtelijke aard mogen worden verwerkt op basis van artikel 10 AVG jo. artikel 32 sub f Uitvoeringswet AVG jo. artikel 89 AVG. De verwerking is noodzakelijk met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig artikel 89, eerste lid van de verordening, en er is voldaan aan de voorwaarden bedoeld in artikel 24 Uitvoeringswet AVG) onderdelen b tot en met d (artikel 32 Uitvoeringswet AVG).

Artikel 24 Uitvoeringswet AVG

Artikel 24 van de Uitvoeringswet AVG stelt als voorwaarden dat:

- a. de verwerking noodzakelijk is met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig artikel 89, eerste lid, van de verordening;

Het CBS verwerkt conform zijn wettelijke taak gegevens alleen voor wetenschappelijk onderzoek of statistische doeleinden. Het CBS heeft extra procedurele en beveiligingsmaatregelen genomen om het gebruik van bijzondere persoonsgegevens te beperken tot een minimum, zoals een additionele verplichte en expliciete goedkeuring. Dit houdt in dat er een passieve toestemming geldt voor vertrouwelijke gegevens en een actieve toestemming voor bijzondere - en strafrechtelijke gegevens. Elk bestand heeft een eigenaar en die geeft toestemming voor het gebruik hiervan.

Standaard in het proces wordt afgewogen of het doel bereikt kan worden met een verwerking van minder of geen persoonsgegevens in de zin van de AVG. Ook wordt het doel van de verwerking beoordeeld.

Daarnaast worden de persoonsgegevens bij binnenkomst zo snel als mogelijk is ontdaan van direct identificerende gegevens zoals naam, adres en woonplaats. Het Burgerservicenummer (BSN) wordt versleuteld (gepseudonimiseerd). De analyses worden alleen uitgevoerd op de gepseudonimiseerde bestanden.

- b. het onderzoek, bedoeld in onderdeel a, een algemeen belang dient;

In de Memorie van Toelichting bij de CBS-wet (Tweede Kamer, vergaderjaar 2001–2002, 28 277, nr. 3, toelichting bij artikel 35, p. 35) is overwogen dat “In het algemeen kan worden gesteld dat het CBS met de uitoefening van zijn taak een zwaarwegend algemeen belang dient.”. Tevens wordt gesteld dat de CBS-wet voldoende passende waarborgen bevat om de privacy van natuurlijke personen te beschermen. Hierbij wordt verwezen naar artikel 37 CBS-wet met betrekking tot het gebruik van gegevens en de openbaarmaking. Op grond van deze bepaling is openbaarmaking van persoonsgegevens door het CBS uitgesloten.

- c. het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning kost; en

Het CBS maakt gebruik van verschillende registers en enquêtes als bron. In de CBS-wet is opgenomen dat het CBS het recht en ook de plicht heeft om gegevens uit deze registers te gebruiken voor statistische en wetenschappelijke doeleinden (artikel 33 CBS-wet). Het voorgaande en de hoeveelheid betrokkenen van wie het CBS persoonsgegevens dient te verwerken voor zijn wettelijke taak heeft tot gevolg dat het vragen van uitdrukkelijke toestemming van betrokkenen een onevenredige inspanning zou kosten.

- d. bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.

Hier voldoet het CBS onder meer aan door technische, organisatorische en wettelijke maatregelen als adequate beveiliging (zie punt 8 en 17), dataminimalisatie en een wettelijke verbod op openbaarmaking van persoonsgegevens.

13. Doelbinding



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

De gegevens mogen alleen voor statistisch of wetenschappelijk onderzoek worden verwerkt. Gebruik van de gegevens voor fiscale, administratieve, controle en gerechtelijke doeleinden is niet toegestaan (artikel 37 lid 1 CBS-wet).

Als verlengde doelen wordt gezien alle verwerkingen welke gericht zijn op het verbeteren van de kwaliteit van de statistiek en het onderzoek naar opzet van nieuwe statistieken of nieuwe statistische processen.

Om de gegevens voor statistiek te mogen gebruiken verwijst artikel 5 lid 1 sub b AVG naar artikel 89 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, zoals de verRIN-procedure en controle op onthullingsrisico's.

14. Noodzaak en evenredigheid



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

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

Algemeen

De gegevens die het CBS ontvangt zijn noodzakelijk voor de vervulling van de wettelijke taak die aan het CBS is opgedragen. Zonder de gegevens kan het CBS zijn bij wet geregelde taak niet uitvoeren.

Omdat gegevens bij publicatie nooit te herleiden zijn naar een individu, worden individuen nooit direct of indirect aangesproken als gevolg van de bewerkingen.

Bij de uitvraag van gegevens en de verwerking daarvan is altijd sprake van dataminimalisatie in de zin van de AVG. Zo is bij de uitvraag van GGZ diagnosegegevens vastgelegd voor welk specifiek doel of doelen de gegevens nodig zijn.

Standaard in het proces wordt afgewogen en beoordeeld of het doel (de betreffende statistiek of het beoogde onderzoek) bereikt kan worden met een verwerking van minder of geen persoonsgegevens.

Proportionaliteit

Er moet worden beoordeeld of de gegevensverwerking evenredig is met het belang van het doel van het onderzoek. Als er geen sprake is van evenredigheid, dient te worden beoordeeld of door het nemen van compenserende maatregelen de evenredigheid kan worden hersteld; er moet sprake zijn van een 'fair balance' tussen het algemeen belang om in casu het onderzoek uit te voeren en de belangen van de betrokkenen.³ In het algemeen geldt dat hoe groter het belang dat met de gegevensverwerking is gediend, hoe groter de inbreuk op de rechten en vrijheden van de betrokkene mag zijn.

Het verzamelen en verwerken van GGZ diagnosegegevens voor statistische en wetenschappelijke doeleinden dient een zwaarwichtig maatschappelijk belang. Zonder de uitvraag van deze gegevens kunnen een aantal basale ontwikkelingen in de GGZ niet in kaart gebracht worden. Dit heeft gevolgen voor mogelijkheden tot beleidsontwikkeling en –monitoring m.b.t. de GGZ, het verkrijgen van het inzicht in doelmatigheid en effectiviteit en het verrichten van onderzoek ter bevordering van de geestelijke gezondheidszorg.

Artikel 5 lid 1 sub c AVG bepaalt dat de gegevensverwerking toereikend, ter zake dienend en beperkt moet zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Dit wordt ook wel het principe van 'minimale gegevensverwerking' genoemd. Om 'noodzakelijk' te zijn moet aan twee voorwaarden zijn voldaan:

- Geschiktheid: De gegevensverwerking is geschikt om het doel te bereiken, en
- Subsidiariteit: Er is geen ander, minder vergaand, middel beschikbaar dat even effectief is.

Geschiktheid

De GGZ diagnosegegevens ten behoeve van statistisch en wetenschappelijk werden tot een paar jaar geleden op gedetailleerd niveau geleverd door de NZa, als onderdeel van de DBC's GGZ. Op basis van deze data zijn statistieken over de behandelde problematiek in de GGZ samengesteld en is wetenschappelijk onderzoek gefaciliteerd. Sinds 2017 was diagnoseinformatie alleen nog beschikbaar op hoofdgroepniveau, tot en met de eerste twee jaar van het Zorgprestatie-model (2023). In overleg met ZIN, TRIMBOS en RIVM is een minimale mate van detail in de diagnoseinformatie gedefinieerd die noodzakelijk is om de wettelijke taken te kunnen vervullen en zinvol onderzoek te verrichten. Het aantal diagnosecodes dat wordt uitgevraagd is gereduceerd ten opzichte van de eerdere datalevering (tot 2017) door NZa. Daarmee is invulling gegeven aan de eis m.b.t. dataminimalisatie. Er is geen reden om te twijfelen aan de geschiktheid van de gegevens en de gebruikte methoden en technieken voor het doel van de onderzoeken.

Subsidiariteit

³ European Data Protection Supervisor (EDPS): Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11 April 2017, pagina 5: "for a measure

Voor het kunnen uitvoeren van de wettelijke taken van het CBS is er geen ander minder vergaand beschikbaar middel beschikbaar dat even effectief is. De reden hiervoor is dat er op het noodzakelijke detailniveau geen andere databronnen beschikbaar zijn. Hierdoor resteert als enige optie een uitvraag bij de GGZ-zorgaanbieders. Er is onderzocht in hoeverre er synergie te bereiken viel door de uitvraag te combineren met de resterende gegevensverzameling door de NZa. Juridisch bleek dit echter niet haalbaar.

15. Rechten van de betrokkene



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.

In artikel 44 Uitvoeringswet AVG wordt een uitzondering gemaakt voor wetenschappelijk onderzoek en statistiek. Indien een verwerking wordt verricht door instellingen of diensten voor wetenschappelijk onderzoek of statistiek, en de nodige voorzieningen zijn getroffen om te verzekeren dat de persoonsgegevens uitsluitend voor statistische of wetenschappelijke doeleinden kunnen worden gebruikt, kan de verwerkingsverantwoordelijke artikel 15, (recht van inzage van de betrokkene) artikel 16(recht op rectificatie), artikel 18 (recht op beperking van de verwerking) en artikel 21 (recht van bezwaar) van de AVG buiten toepassing laten.

Betrokkenen, waarvan het CBS de gegevens via GGZ-zorgaanbieders ontvangt, worden door het CBS niet direct geïnformeerd over de gegevensverwerking op grond van de uitzondering van artikel 14 lid 5 sub b AVG. Reden hiervoor is dat het CBS gebruik maakt van verschillende registers en enquêtes als bron en dat in de CBS-wet is opgenomen dat het CBS het recht (en de plicht) heeft om gegevens uit deze registers te gebruiken voor statistische en wetenschappelijke doeleinden artikel 33 CBS-wet. Het informeren van deze indirecte betrokkenen zou dan een onevenredige inspanning vergen.

Betrokken GGZ zorgaanbieders worden actief door het CBS geïnformeerd middels een informatiebrief die bij de informatie-uitvraag wordt geleverd. Hierbij wordt ook verwezen naar de website van het CBS, de onderzoeksopzet, de ingezette bronnen en is er een helpdesk beschikbaar voor vragen over het onderzoek.

Gelet op artikel 14 lid 5 sub b AVG is het CBS wel gehouden om informatie over zijn verwerkingsactiviteiten openbaar te maken en daaraan voldoet het CBS middels een bronnenregister en door het publiceren van informatie over het statistische proces op de website van het CBS. Ook wordt bij publicatie van statistische informatie de bronnen welke geleid hebben tot deze informatie opgenomen.

Op de website staat een privacyverklaring en uitleg over het inzagerecht opgenomen.

C. 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 zelf.

16. Risico's



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

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

Ad a.

De verwerkingen dienen uitsluitend statistische doeleinden en hebben daardoor geen negatieve gevolgen voor de rechten en vrijheden van betrokkenen (behandelde personen en zorgaanbieders) omdat het doel altijd aggregaten zijn waaraan geen gegevens over afzonderlijke personen kunnen worden ontleend. Er is alleen een risico op een datalek, een potentieel risico met hoge impact.

Ad b. Medewerkers die over de gegevens kunnen beschikken, dan wel externe oorzaken van een datalek.

Ad c en ad d. Na het nemen van de benodigde maatregelen resteert een acceptabel restrisico.

Risico's

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

1.	
Categorie	Schade / maatschappelijk nadeel
Incident	Datalek (interne omgeving of remote acces omgeving CBS): persoonsgegevens beschikbaar voor derden
Impact op betrokkene	Hoog
Kans	Laag
Risico	Laag
Aanbevolen maatregelen	Zowel in de breedte (veel al dan niet gevoelige gegevens) als in de diepte (veel personen) heeft het CBS de beschikking over risicovolle informatie zodat de privacy impact ingeval van een datalek hoog kan zijn. Er zijn echter conform ISO 27001 mede gelet op het potentieel hoge risico passende technische en organisatorische beveiligingsmaatregelen getroffen en bovendien zijn alle verwerkingen van het CBS zo ingericht dat de kans op herkenning of herleidbaarheid van een individu minimaal is. Daarmee is het risico voor de betrokkene zo veel mogelijk ingeperkt.
Actiehouder	CBS
Impact na maatregelen	Laag

2.	
Categorie	Schade / maatschappelijk nadeel
Incident	Stigmatisering als gevolg van datalek
Impact op betrokkene	Hoog
Kans	Laag
Risico	Laag

Aanbevolen maatregelen	Zowel in de breedte (veel al dan niet gevoelige gegevens) als in de diepte (veel personen) heeft het CBS de beschikking over risicovolle informatie zodat de privacy impact ingeval van een datalek hoog kan zijn. Er zijn echter conform ISO 27001 mede gelet op het potentieel hoge risico passende technische en organisatorische beveiligingsmaatregelen getroffen en bovendien zijn alle verwerkingen van het CBS zo ingericht dat de kans op herkenning of herleidbaarheid van een individu minimaal is. Daarmee is het risico voor de betrokkene zo veel mogelijk ingeperkt.
Actiehouder	CBS
Impact na maatregelen	Laag

D. Beschrijving voorgenomen maatregelen

In onderdeel D wordt gezien 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 PIA is, als het gaat om beveiligingsmaatregelen, expertise over informatiebeveiliging belangrijk.

17. 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.

Op basis van de CBS-brede risicoanalyse uit 2015 wordt geconcludeerd dat het CBS op grond van de criteria die in de VIR-BI 2013 zijn genoemd het vertrouwelijkheidsniveau Departementaal Vertrouwelijk (Dep.V.) is. Tevens valt de verwerking van bijzondere persoonsgegevens onder risicoklasse 2 van de Autoriteit Persoonsgegevens.

Voor het vaststellen van de noodzakelijke maatregelen hanteert het CBS de ISO 27001/2 norm en de Baseline Informatiebeveiliging Overheid (BIO) als uitgangspunt. Met de genomen maatregelen zijn de risico's voldoende afgedekt. Volledige afdekking van de risico's zal nooit mogelijk zijn omdat de menselijke factor, veelal de belangrijkste factor bij een beveiligingsincident, nooit volledig is uit te sluiten.

De scope omvat alle primaire en alle ondersteunende processen van het Centraal Bureau voor de Statistiek en de daarvoor gebruikte informatiesystemen, waarbij onder informatiesysteem wordt verstaan: het samenhangend geheel van gegevensverzamelingen en de daarbij behorende personen, procedures, processen en programmatuur, alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.

De beveiligingsprocedures vallen binnen de directe verantwoordelijkheid van het lijnmanagement. Het CBS controleert periodiek op naleving van de betrouwbaarheidsmaatregelen:

- Ieder kwartaal wordt er een rapportage opgesteld met daarin de meldingen rondom privacy en security.
- Tweejaarlijks wordt een externe IT-beveiligingsaudit uitgevoerd.

De ISO-27001 certificering van het gehanteerde managementsysteem voor informatiebeveiliging. Het certificaat staat op de website van het CBS.

Het CBS heeft de maatregelen ten aanzien van de beveiliging vastgelegd in de procesdocumentatie en deze zijn juist, volledig en up-to-date.

Met betrekking tot het personeel:

- alle CBS-medewerkers en stagiairs hebben een geheimhoudingsverklaring ondertekenend waarin de verplichtingen en verantwoordelijkheden met betrekking tot geheimhouding zijn vastgelegd;
- personeelsleden van het CBS zijn ambtenaren en dus gehouden om alle informatie die door hun werkzaamheden tot hun kennis komt als vertrouwelijk te behandelen. Daarnaast hebben ze een eed of belofte afgelegd en een verklaring met de eed of belofte ondertekend;
- tijdelijke externe medewerkers, uitzendkrachten en stagiaires tekenen eveneens een geheimhoudingsverklaring, maar leggen geen eed of belofte af aangezien het geen aanstelling als ambtenaar betreft;
- van derden worden geheimhoudingsverklaringen verlangd;
- geheimhouding wordt in voorkomende gevallen vastgelegd in overeenkomsten met derde organisaties (zoals wetenschappelijke instellingen) die toegang krijgen tot persoonsgegevens;

De wijze waarop microbestanden zijn beveiligd bij het gebruik van Remote Access is in de [Richtlijnen voor Remote Access-output](#). Daarnaast heeft het CBS [regels](#) voor het gebruik van de Remote Access faciliteit, een [maatregelenbeleid](#) en legt het voorwaarden voor het gebruik van de Remote Access faciliteit vast in een projectovereenkomst.

Vooraf aan iedere verwerking wordt er een risicoanalyse uitgevoerd op de privacy en beveiligingsaspecten. Dit gebeurt aan de hand van een Baseline(toets) privacybescherming en informatiebeveiliging. Doel van deze toets is om vast te stellen of voor een onderhavig proces voldoende maatregelen genomen zijn om risico's, op het gebied van privacybescherming en informatiebeveiliging, tot een aanvaardbaar niveau te reduceren. Met andere woorden of het proces voldoet aan de eisen van privacy- en beveiligingsnormen.

Het eerste deel van de toets is een checklist waarin een aantal normen op het gebied van privacybescherming en informatiebeveiliging is opgenomen (baseline). Hier wordt beoordeeld of er wordt voldaan aan de gestelde normen en of de bijbehorende beheersmaatregelen correct en volledig zijn uitgevoerd. Het tweede deel van de toets is de vraag of er, in aanvulling op de generieke maatregelen, voor dit proces specifieke maatregelen zijn getroffen (baselinetoets). Specifieke maatregelen kunnen bijvoorbeeld nodig zijn door de aard of de inrichting van het proces of door het aantal personen dat erbij betrokken is. Als er voor het proces specifieke maatregelen zijn getroffen dient op basis van een risicoafweging te worden beargumenteerd dat daarmee de gesignaleerde risico's afdoende zijn afgedekt. De Baselinetoets wordt jaarlijks geëvalueerd.

Het CBS kent naast externe audits ook een systeem van interne audits. Jaarlijks wordt daarover gerapporteerd aan de directie van het CBS.

Tenslotte heeft het CBS een aantal organisatorische maatregelen:

- Alleen de onderzoekers die daadwerkelijk onderzoek doen hebben toegang (krijgen autorisatie) tot de gegevens die nodig zijn voor het onderzoek;
- Autorisatie wordt per onderzoeker en per onderzoek verleend. Voor elk nieuw onderzoek moet een medewerker opnieuw toegang krijgen;
- Gegevens worden pas beschikbaar gesteld nadat een onderzoeksplan is gemaakt (en goedgekeurd) waarin de (project-specifieke) doelbinding en de benodigde gegevens staan beschreven;
- Elk onderzoek moet gepubliceerd worden. Het CBS controleert op onthullingsrisico's om te waarborgen dat er nooit onthulling kan plaats vinden op persoons, huishoudens-en instellingsniveau;
- Dezelfde maatregelen gelden voor de remote acces onderzoekers.

Hier kunt u aanvullende punten toevoegen: selecteer de tab *Invoegen*, kies *Snelonderdelen, Aanvullend punt*

Voeg hier wanneer gewenst een afsluitende alinea toe. Denk bijvoorbeeld aan:

- Lessen uit deze PIA
- Volgende stappen etc.



Maatregelen
nemen
Privacybewustwording
PIA
Doelbinding Noodzaak
Effecten in kaart
Bescherming van
persoonsgegevens
Risico's
minimaliseren
Richtinggevend
Rechtsgrond
Met open vizier