PRIVACY MANAGEMENT PARTNERS

High-pressure DPIA
Covid-19 onderzoek vaccinatie medische risicogroepen

In opdracht van Rijksinstituut voor Volksgezondheid en Milieu

20 april 2021

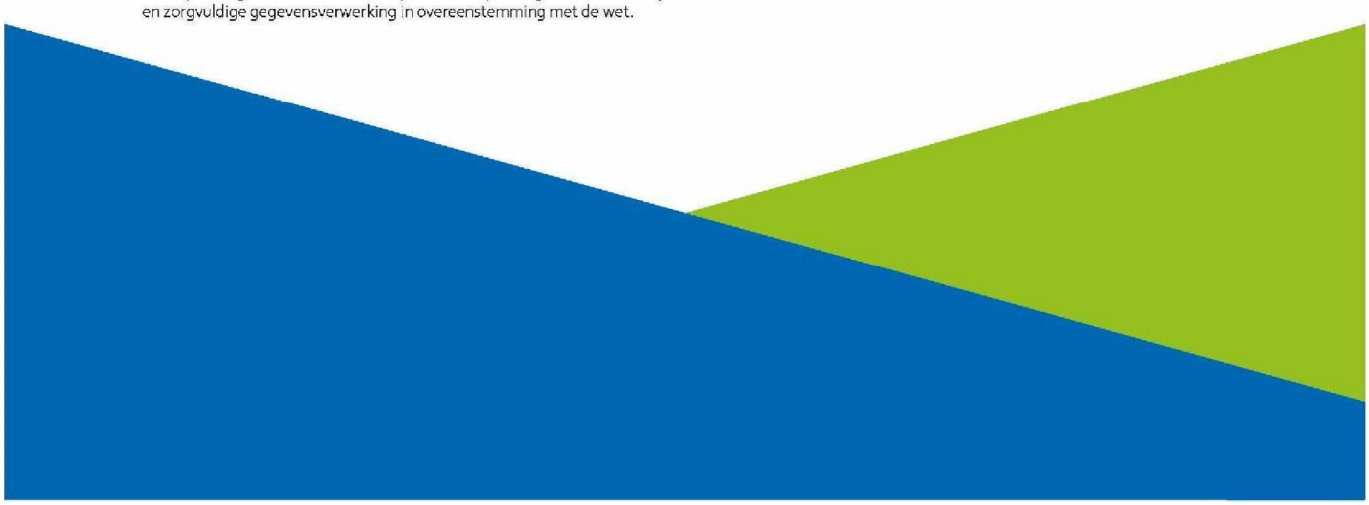
Versie 1.0 (definitief)

High-pressure DPIA
Covid-19 onderzoek vaccinatie medische risicogroepen

In opdracht van Rijksinstituut voor Volksgezondheid en Milieu

Auteurs
Privacy Management Partners
5.1.2e 5.1.2e 5.1.2e 5.1.2e
5.1.2e

20 april 2021



Inhoud

Toelichting high-pressure DPIA

Toelichting

Privacy Management Partners (hierna: PMP) heeft de high-pressure DPIA methodiek ontwikkeld als 'light' variant van de normale DPIA om in korte tijd de stand van zaken op het gebied van privacycompliance van een (toekomstige) verwerking in kaart te brengen. Daarbij wordt uitsluitend uitgegaan van de informatie die door de opdrachtgever en/of derden is aangeleverd. Indien daar op een later tijdstip aanleiding toe is, kan deze high-pressure DPIA als input dienen om het Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA) verder te completeren.

Deze high pressure DPIA functioneert als een **haalbaarheidstoets** in het licht van privacy- en gegevensbeschermingseffecten van het Covid-19 onderzoek vaccinatie medische risicogroepen, waarbij gebruik wordt gemaakt van een koppeling van verschillende bronbestanden: Osiris, Vaccinatieregister (CIMS), CoronIT, Vektis, NICE en data van het CBS. Ter voorbereiding van het onderzoek wil het RIVM graag inzichtelijk hebben welke mogelijke risico's er voor betrokkenen kunnen zijn bij het uitvoeren van dit onderzoek. Daarnaast heeft het RIVM ook gevraagd om expliciet in kaart te brengen welke juridische grondslagen er zijn om de uitvraag van de gegevens bij de andere partijen mogelijk te maken en te kunnen verantwoorden. Deze hoofdvragen worden meegenomen in dit rapport.

DISCLAIMER
Deze high-pressure DPIA mag niet worden opgevat als een DPIA in de zin van artikel 35 AVG.
De reden dat geen 'normale' DPIA is uitgevoerd, is omdat in deze fase van het project de omstandigheden van de gegevensverwerking nog onvoldoende concreet zijn om beoordeeld te worden. Het is derhalve raadzaam om te zijner tijd deze DPIA bij te werken als het project meer handen en voeten heeft gekregen.

Leeswijzer

Deze DPIA bestaat uit een beschrijving van de gegevensverwerking en een overzicht risicotabel. In hoofdstuk 1 wordt beschreven wat het belang van het onderzoek, de werking van de RA-omgeving van het CBS, de categorieën persoonsgegevens, de mogelijke grondslag voor dit onderzoek en de rollen en verantwoordelijkheden van de verschillende partijen is.
In hoofdstuk 2 zijn een aantal risico's geïdentificeerd en geven we een aantal aandachtspunten voor de verdere uitwerking van dit project.

1 Beschrijving onderzoek

1.1 Belang onderzoek

Op dit moment zijn er ruim 2 miljoen vaccinaties gezet om burgers te beschermen tegen COVID-19. De effectiviteit en de duur van bescherming is voor verschillende medische risicogroepen vooralsnog niet bekend. Hervaccinatie zou dan ook nodig kunnen zijn voor medische risicogroepen. Dit houdt ook in dat deze kwetsbare groepen mogelijk nog langdurige stringente maatregelen ter preventie van infectie zullen moeten hanteren.

Het onderzoeksvoorstel is daarom ook opgesteld met het doel om continu inzicht te hebben in de ziektelast bij een vaccinatiegraad van verschillende medische risicogroepen tijdens de COVID-19 epidemie om daarmee doorlopend:

- de vaccineffectiviteit vast te kunnen stellen,
- de vaccinatieprioritering aan te kunnen passen,
- te bepalen voor welke (sub)risicogroepen aanpassing van beschermingsmaatregelen mogelijk wordt, en
- te bepalen hoe COVID-19 (na)zorg dient te worden vormgegeven.

Het onderzoek zal 4 jaar duren. De bevindingen van dit onderzoek dienen als input voor het bijsturen van het bestrijdings- en zorgmanagementbeleid en zijn daarmee van belang voor de algehele volksgezondheid en bescherming van medische risicogroepen.

1.2 Opzet van het onderzoek

Voor dit 4-jaar durende onderzoek zullen de volgende bestanden aan elkaar gekoppeld worden:

- Vanuit het RIVM:

- OSIRIS, het generieke informatiesysteem van het RIVM waarin meldingsplichtige infectieziekten ex art. 28 Wet publieke gezondheid worden geregistreerd. In OSIRIS zijn vanaf het begin van de epidemie door de GGD persoonsgegevens ingevoerd van alle positief geteste personen die door laboratoria gemeld werden bij de GGD. Na de start van de vaccinaties zal in OSIRIS ook informatie beschikbaar zijn over de vraag of een geteste persoon gevaccineerd was of niet. Hierdoor wordt het mogelijk voor grotere groepen patiënten te bepalen of er sprake is van vaccinfalen en kunnen preventie-strategieën of de strategie voor hervaccinatiecampagnes worden aangescherpt.

- CIMS, het COVID-vaccinatie informatie- en monitoringsysteem ('vaccinatieregister'), waarin gegevens over de COVID-19-vaccinatie bijgehouden. In het CIMS staan van iedere gevaccineerde persoon geregistreerd: voor- en achternaam, adresgegevens, geboortedatum, BSN, reden vaccinatie (leeftijd / medische aandoening / zorgmedewerker), datum en plaats waar de vaccinatie is gegeven, en de naam van het vaccin en het batchnummer. Om de vaccineffectiviteit te bepalen moet het vaccinatieregister gekoppeld worden aan de testgegevens in OSIRIS.

- Vanuit Vektis:

- Gegevens over de zorgconsumptie (declaratiegegevens), waaronder medicatiegegevens. Het betreft zowel gegevens van vóór de Covid-19 pandemie als van daarna. De Vektis dataset helpt om te bepalen wat de zorgconsumptie vóór de COVID-19 infectie was en wat de

zorgconsumptie post-COVID-19 is om zo inzicht te verkrijgen over het optreden van complicaties inclusief de zorgbehoefte daarbij tijdens herstel per risicogroep.

Vanuit Vektis bestaat al een (jaarlijkse) datastroom richting het CBS, die op verzoek wordt aangevuld met extra leveringen. Via het beveiligde dataportaal van Vektis worden gegevens op BSN niveau gedeeld met het CBS die vervolgens zorgdragen voor het pseudonimiseren/versleutelen van deze gegevens (verrinnen).

- Vanuit de Stichting Nationale Intensive Care Evaluatie (NICE):
  - De Covid-registratie: Het aantal ziekenhuisopnames, IC opnames, de opnameduur en het BSN. Deze dataset, die momenteel dagelijks aan het RIVM wordt geleverd, staat toe te zien wie er van de positief geteste personen uiteindelijk is opgenomen in het ziekenhuis of IC, hoe lang de opname was en wie er tijdens de opname overleed.

  - De reguliere NICE-registratie (MDS) met klinische data van alle IC-patiënten incl. COVID-19 patiënten op de IC.

- Vanuit het CBS:
  - Socio-demografische kenmerken. Deze zijn nodig voor de bepaling van zowel COVID-19 gerelateerde aspecten (overlijden tijdens ziekte of juist in de herstelfase na opname vanwege COVID-19) als van mogelijke bijdragende aspecten voor virus-expositie en beloop van ziekte (gezinsgrootte, zwangerschap/recente geboorte, sociaal-economische status).

  - Het is de bedoeling dat de gegevens uit CoronIT door de GGD's worden aangeleverd bij het CBS.[1] Deze dataset geeft informatie om te kunnen bepalen hoe vaak verschillende personen/risicogroepen getest worden (identificatie van de risicogroepen d.m.v. koppeling met de Vektis-dataset) en wie er uiteindelijk positief was of opnieuw positief werd (herinfectie).

NB. Wij merken op dat de gegevens die reeds door NICE (Covid registratie) en de GGD GHOR (CoronIT) worden aan het RIVM worden geleverd *los van dit onderzoek*, reeds gegevens *van het RIVM* zijn geworden (via een zogeheten 'derdenverstrekking'). Het zijn dus RIVM-data, geen NICE-data of GGD GHOR-data. Het RIVM kan AVG-technisch daarom zelfstandig beslissen om deze gegevens ter beschikking te stellen voor dit project. NICE en de GGD GHOR hebben AVG-technisch geen rol bij het gebruik van deze gegevens.

1.3 Categorieën persoonsgegevens

Voor dit onderzoek worden verschillende categorieën persoonsgegevens gebruikt, waaronder bijzondere persoonsgegevens zoals gezondheidsgegevens.

Het van belang om te weten dat op het moment van schrijven van deze DPIA het onderzoek nog in de opzetfase staat. De onderzoeksvragen moeten nog verder geconcretiseerd worden. De categorieën persoonsgegevens hangen dan ook af van de definitieve opzet. In onderstaande tabel worden de persoonsgegevens benoemd die de partijen **verwachten** te gebruiken voor dit onderzoek en welke hiervan als gevoelig of bijzonder beschouwd kunnen worden.

[1] Is thans nog niet gerealiseerd.

Tabel 1: categorieën persoonsgegevens

Partij	Categorie gegevens	Typering persoonsgegevens
RIVM *(Osiris, CIMS)*	BSN	Wettelijk identificerend nummer (verhoogd gevoelig)
	Geslacht	Gewoon persoonsgegeven
	Geboortejaar	Gewoon persoonsgegeven
	Postcode 4-cijferig	Gewoon persoonsgegevens
	Vaccinatiegegevens (waaronder productnaam en batchnummer van de vaccinatie(s), datum vaccinatie(s), uitvoerende instantie)	Bijzondere persoonsgegevens
	Testdatum	Gewoon persoonsgegevens
	Testuitslag	Bijzonder persoonsgegeven
CBS	BSN	Wettelijk identificerend nummer (verhoogd gevoelig)
	Overlijdensdatum	Geen persoonsgegeven
	Doodsoorzaak	Geen persoonsgegeven[2]
	Gezinsgrootte	Gewoon persoonsgegeven
	Zwangerschap	Bijzonder persoonsgegeven
	Geboortedatum	Gewoon persoonsgegeven
	Sociaal economische status (SES)	Gewoon persoonsgegeven (mogelijk verhoogd gevoelig)
	Land van herkomst	Bijzonder persoonsgegeven
	Opleidingsniveau	Gewoon persoonsgegeven
	Indien mogelijk: (tijdelijk) baanverlies/uitkering na Covid-19 infectie	Gewoon persoonsgegeven (mogelijk verhoogd gevoelig)
NICE[3]	BSN	Wettelijk identificerend nummer (verhoogd gevoelig)
	Geslacht	Gewoon persoonsgegeven
	Geboortejaar	Gewoon persoonsgegeven
	Postcode 4-cijferig	Gewoon persoonsgegeven
	Co-morbiditeit bij opname	Bijzonder persoonsgegeven
	Gebruikte medicatie voor opname	Bijzonder persoonsgegeven
	Ziekenhuisopname	Bijzonder persoonsgegeven
	Opnameduur	Bijzonder persoonsgegeven
	IC opnames	Bijzonder persoonsgegeven
	Overlijden	Geen persoonsgegeven

[2] NB. Intern beschouwt het CBS doodsoorzaak als bijzonder persoonsgegeven. Die buitenwettelijke kwalificatie, die voortkomt uit de zorgvuldigheidseisen van de Wet CBS, staat echter niet in de weg aan onze conclusies over de AVG of de risico's voor de betrokkenen.

[3] NB. NICE levert twee datasets aan:

1) de COVID-registratie, een beperkte set over COVID-19 op de IC en afdeling incl. BSN en opname/ontslagdatum en overlijden) en

2) de reguliere NICE-registratie, te weten: klinische data van alle IC-patiënten incl. COVID-patiënten op de IC.

Vektis	BSN	Wettelijk identificerend nummer (verhoogd gevoelig)
	Geslacht	Gewoon persoonsgegeven
	Geboortejaar	Gewoon persoonsgegeven
	Postcode 4-cijferig	Gewoon persoonsgegeven
	Zorggebruik op basis van declaratiegegevens: Gebruik van medicatie bij risicogroepen voorafgaande aan COVID-19 pandemie alsmede na een COVID-19 infectie (zoals recente chemotherapie, hart- en longmedicatie, insuline/orale antidiabetica, verschillende soorten immuunsuppressiva)	Bijzondere persoonsgegevens

1.4 CBS waarborgen informatiebeveiliging

1.4.1 Werking Remote Access (RA) omgeving

In deze paragraaf wordt de RA omgeving toegelicht.[4]

De partijen kunnen hun bronbestanden uploaden via de beveiligde portal van CBS. De bestanden zullen dan eerst naar een zeer beveiligde, specialistische afdeling gestuurd worden binnen het CBS om de encryptie uit te voeren op alle persoonsdatabestanden. Op deze afdeling worden de bestanden onder andere 'verRINd'. Dit houdt in dat de data wordt versleuteld met een uniek RIN nummer, op basis van specifieke koppeldata zoals het BSN nummer. Het verrinnen gebeurt automatisch. Mochten er "missings" zijn, dan onderzoeken de CBS medewerkers op basis van hun expertise of deze alsnog gekoppeld kunnen worden.

Wanneer de data is versleuteld, wordt de gepseudonimiseerde data beschikbaar gesteld in de RA-omgeving. De RA-omgeving bestaat al een langere tijd en is een instrument van het CBS om op een veilige manier met andere partijen onderzoek uit te kunnen voeren. Alle partijen krijgen een koppelsleutel om hun eigen originele data in te kunnen zien. Van de andere partijen kunnen zij enkel de gepseudonimiseerde data inzien.

Op dit moment hebben het RIVM en Vektis al een instellingsmachtiging om te kunnen werken in de RA- omgeving. NICE heeft deze nog niet en zal hier nog een aanvraag voor indienen. Als zij niet in aanmerking komen voor een instellingsmachtiging, dan is het idee dat zij via een detachering bij het RIVM alsnog toegang kunnen krijgen tot de RA-omgeving.

1.4.2 Waarborgen pseudonimisering

Het CBS heeft conform wettelijke eisen van de AVG een proces ingericht om persoonsgevoelige gegevens te pseudonimiseren (verrinnen). Het CBS heeft organisatorisch, infrastructureel en procesmatig gewaarborgd dat depseudonimisering alleen bij hoge uitzondering en op heel gecontroleerde wijze kan plaatsvinden. Het aantal CBS-medewerkers dat bevoegd is deze handeling uit te voeren is zeer beperkt (<5).

[4] Zie ook: https://www.digitaleoverheid.nl/praktijkvoorbeeld-centraal-bureau-voor-de-statistiek-cbs/

1.5 Juridisch kader

1.5.1 Verwerkingsverantwoordelijke

RIVM: Omdat het RIVM een dienst is van het ministerie van VWS, is de Minister van VWS de verwerkingsverantwoordelijk voor dit onderzoek.

NICE: Voor zover NICE alleen leverancier is van de dataset, heeft zij **geen AVG-rol** in dit onderzoek. (NB. NICE R&S / KIK-AMC is verwerker voor de persoonsgegevens die zullen worden aangeleverd).
NB. Dit is alleen anders als de stuurgroep (mede) het doel en de middelen van de gegevensverwerking in dit project bepaalt. In dat geval is NICE medeverantwoordelijke voor de gegevensverwerkingen in dit project. Dit zou kunnen worden ondervangen door in het onderzoeksprotocol het RIVM aan te wijzen als projectleider en dus degene die inhoudelijk de beslissingen neemt, en daar waar nodig de stuurgroep informeert of daarin afstemming zoekt.

Vektis: Voor zover Vektis alleen leverancier is van de dataset, heeft zij geen AVG-rol in dit onderzoek. (NB. Vektis is verwerker voor de persoonsgegevens die zullen worden aangeleverd.)
NB. Dit is alleen anders als de stuurgroep (mede) het doel en de middelen van de gegevensverwerking in dit project bepaalt. In dat geval is Vektis medeverantwoordelijke voor de gegevensverwerkingen in dit project. Dit zou kunnen worden ondervangen door in het onderzoeksprotocol het RIVM aan te wijzen als projectleider en degene die inhoudelijk de beslissingen neemt, en daar waar nodig de stuurgroep informeert of daarin afstemming zoekt.

NB. Voor zowel NICE als Vektis geldt dat zij een onderzoeker (promovendus) zullen leveren. Dit maakt hen echter nog niet per se tot verwerkingsverantwoordelijke voor de gegevensverwerking in het kader van dit onderzoek. Dat is pas het geval als die onderzoekers ook *bij NICE c.q. Vektis* aan de slag gaan. Echter, als de onderzoekers worden gestationeerd bij het RIVM (al dan niet via detachering), dan hebben NICE en Vektis geen AVG-rol bij dit onderzoek. (Als de promovendi bij een universiteit aan de slag gaan, dan is de universiteit (ook) verwerkingsverantwoordelijke voor dit onderzoek). Om de zaken overzichtelijk te houden met AVG-technisch zo weinig mogelijk rompslomp, ligt een aanstelling/detachering van de promovendi bij het RIVM voor de hand (dat staat AVG-technisch los van de financiering).

CBS: Ook het CBS levert een dataset. Daarnaast beheert het CBS de RA-omgeving. Volgens het CBS is het CBS verwerkingsverantwoordelijke voor de RA-omgeving. Het CBS wijst daarbij op art. 41 e.v. Wet CBS. Indien we meegaan in deze redenering, is het CBS **medeverwerkingsverantwoordelijke** voor het onderzoek, en dient tussen het RIVM en het CBS een art. 26 AVG-regeling te worden getroffen. Wij wijzen erop dat het de partijen vrij staat de invulling van de artikel 26-regeling in te vullen en de AVG-overplichtingen onderling te verdelen. De verantwoordelijkheid van het CBS zou bijvoorbeeld beperkt kunnen blijven tot de verantwoordelijkheid voor de pseudonimisering (verrinnen), de beveiliging van de RA-omgeving en de daarmee samenhangende verplichtingen van de AVG (bijv. naleving van de meldplicht datalekken bij beveiligingsincidenten rondom de RA-omgeving).

NB. De **GGD/GGD-GHOR** heeft geen AVG-rol in dit onderzoek, en wordt enkel over dit onderzoek geïnformeerd, omdat de data die door de GGD bij het RIVM (en straks ook bij het CBS) zijn aangeleverd voor dit onderzoek gebruikt zullen worden.

1.5.2 Grondslag

RIVM: Omdat dit onderzoek plaatsvindt in het kader van de publieke taak van het RIVM, vormt artikel 6(1)(e) AVG de rechtsgrond voor de verwerking van de persoonsgegevens in het kader van het onderzoek. Idem voor het CBS.

De gegevens in OSIRIS kunnen gebruikt worden door het RIVM voor de uitvoering van de wettelijke taken. Dat geldt ook voor gebruik van de gegevens voor wetenschappelijk onderzoek voor zover dit onderzoek plaatsvindt op grond artikel 3, eerste lid, van de Wet op het RIVM. Wel is de afspraak gemaakt dat voor meer fundamenteel wetenschappelijk onderzoek en, in het algemeen, research betaald door onderzoeksfondsen wél toestemming wordt gevraagd van de registratiecommissie. Voor dit project kunnen de gegevens volgens het RIVM gebruikt worden zonder dat de registratiecommissie toestemming daarvoor geeft. Het gaat namelijk om onderzoek dat wordt gedaan op grond van artikel 3, eerste lid, Wet RIVM.

CBS: Omdat de verwerking van de gegevens met behulp van CBS microdata plaatsvindt in de RA-omgeving vormt ook in dit geval artikel 6(1)(e) AVG de grondslag voor de gegevensverwerking

NICE: Omdat NICE verwerker is van de door haar verwerkte gegevens, zal NICE mogelijk toestemming nodig hebben van de ziekenhuizen (de verwerkingsverantwoordelijken voor de NICE data). De Overeenkomst tussen KIK/AMC en het RIVM biedt ruimte voor gebruik zonder toestemming van de ziekenhuizen, maar de interpretatie van artikel 4.2 (gebruik van de gegevens voor Toegestane Doeleinden) laten wij verder aan de partijen bij de overeenkomst.

NB. Omdat het gebruik van persoonsgegevens voor wetenschappelijk onderzoek en statistiek geacht wordt verenigbaar het zijn met het doel waarvoor zij zijn verzameld (art. 5(1)(b) AVG), hebben de ziekenhuizen geen zelfstandige grondslag nodig voor het aanleveren van gegevens (art. 6(4) AVG). De levering zal wel aan de voorwaarden van artikel 89 AVG moeten voldoen.[5]

Verder speelt mogelijk art. 7:458 Burgerlijk Wetboek een rol (gebruik medische gegevens in wetenschappelijk onderzoek of statistiek). In dat geval moet dus kunnen worden beargumenteerd waarom toestemming vragen aan de patiënt in redelijkheid niet mogelijk is. Mogelijk kan hier worden aangesloten bij het standpunt van VWS dat gelet op de druk op de zorg het vragen van toestemming aan de patiënten in redelijkheid niet mogelijk is om het in casu om grote aantallen patiënten betreft.[6] Ook mag de patiënt geen uitdrukkelijk bezwaar hebben gemaakt tegen het gebruik van zijn/haar gegevens in het onderzoek.

Vektis: Omdat Vektis verwerker is van de door haar verwerkte gegevens, zal Vektis instemming nodig hebben van de zorgverzekeraars (de verwerkingsverantwoordelijken voor de Vektis data). Volgens Vektis Omdat het gebruik van persoonsgegevens voor wetenschappelijk onderzoek en statistiek geacht wordt verenigbaar het zijn met het doel waarvoor zij zijn verzameld (art. 5(1)(b) AVG), heeft de zorgverzekeraar geen zelfstandige grondslag nodig voor het aanleveren van gegevens (art. 6(4) AVG).[7] De levering en het gebruik van de gegevens zal wel aan de voorwaarden van artikel 89 AVG moeten voldoen.

---

[5] Voor de volledigheid wijzen wij erop dat voor de verstrekking van gegevens van het RIVM cq CBS door NICE en Vektis geen aparte grondslag in artikel 6(1) AVG hoeft te worden gevonden (zie overweging 50, eerste en tweede volzin). Een verstrekking van persoonsgegevens zonder wettelijke verplichting of toestemming van de betrokkene moet verenigbaar zijn met het doel waarvoor de gegevens zijn verzameld (art. 5(1)(b) juncto art. 6(4) AVG). Maar omdat artikel 5(1)(b) stelt dat gebruik van gegevens voor wetenschappelijk onderzoek en statistiek geacht wordt verenigbaar te zijn, kan artikel 6(4) AVG in casu buiten toepassing worden gelaten, mits de waarborgen als vereist door artikel 89 AVG en eventueel art. 24 UAVG en -in geval van gegevens waarop het medisch beroepsgeheim van toepassing is- art. 7:458 BW zijn toegepast.

[6] Zie ook: https://www.datavoorgezondheid.nl/wegwijzer-ai-en-corona/vraag-en-antwoord/wanneer-en-hoe-kan-ik-gebruik-maken-van-de-wettelijk-uitzonderingen-voor-het-vragen-van-toestemming-i.r.t.-wetenschappelijk-onderzoek

[7] Zie voetnoot 1.

Niettemin geldt zowel voor NICE als voor Vektis dat de koninklijke weg die van een wettelijke regeling is, die dwingt tot het vrijgeven van de gegevens -inclusief BSN- aan het RIVM, waardoor ook het probleem van de instemming door de achterliggende verwerkingsverantwoordelijken wordt weggenomen. Daarnaast kunnen in de regeling ook waarborgen worden opgenomen ter bescherming van de belangen van de betrokkenen.

1.5.3 Bijzondere gegevens

Op grond van art. 9(1) AVG is de verwerking van bijzondere gegevens in beginsel verboden. Art. 24 UAVG vormt een uitzondering op dit verbod voor wetenschappelijk onderzoek en statistiek, mits aan een viertal voorwaarden is voldaan:

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

Ad 1) In het grondrechtenrecht, waartoe ook de AVG behoort, wordt 'noodzakelijkheid' uitgelegd als:

- effectiviteit (een geschikt middel), én
- subsidiariteit (er kan niet worden volstaan met minder data).

Dit betekent dat tijdens het onderzoek steeds moet worden gevalideerd of de diverse datasets een wezenlijke bijdrage leveren aan het onderzoek. Op het moment dat blijkt dat bepaalde data niet noodzakelijk zijn, moet de dataset worden aangepast.

Ad 2) Wij bevestigen dat het onderhavige onderzoek het algemeen belang dient (volksgezondheid en beleid).

Ad 3) Wij wijzen erop dat alvorens met het onderzoek wordt aangevangen, het RIVM onderbouwt waarom het vragen van toestemming onmogelijk is dan wel een onevenredige inspanning kost. Er kan worden gedacht aan de situatie dat het niet altijd mogelijk is de betrokkene te achterhalen. Ook zijn er gevallen waarin het theoretisch mogelijk zou zijn om de betrokkene op de hoogte te stellen, maar waarbij de vereiste inspanning in geen verhouding staat tot het doel dat daarmee wordt gediend. Hierbij kan tevens spelen dat op dit moment de druk op de gezondheidszorg dusdanig groot is dat toestemming vragen onevenredig kan worden geacht.[8]

Ad 4) Omdat het onderzoek nog in ontwikkeling is, kunnen op dit moment nog geen beoordeling worden gemaakt van de waarborgen. Wel weten we dat de RA-omgeving van het CBS door de onderzoekers gebruikt zal worden en dat de gegevens worden gepseudonimiseerd met behulp van de verRIN-procedure van het CBS. Maar ook daarbuiten dienen de nodige waarborgen genomen te

[8] Zie ook: https://www.datavoorgezondheid.nl/wegwijzer-ai-en-corona/vraag-en-antwoord/wanneer-en-hoe-kan-ik-gebruik-maken-van-de-wettelijk-uitzonderingen-voor-het-vragen-van-toestemming-i.r.t.-wetenschappelijk-onderzoek

worden, met name op het gebied van dataminimalisatie (noodzakelijkheid van de gegevens), bewaartermijnen, datakwaliteit, geheimhouding/vertrouwelijkheid en transparantie (privacyverklaring).

1.5.4 BSN

Data in CoronIT worden door GGD GHOR[9] op basis van de Wet publieke gezondheid doorgegeven aan het RIVM, maar zonder BSN. CoronIT data mét BSN worden door GGD GHOR wel aan het CBS geleverd. Ook NICE en Vektis zullen hun gegevens aanleveren op basis van het BSN. Vanwege het belang van unieke identificeerbaarheid in de (gepseudonimiseerde) onderzoekspopulatie, is het van belang om deze bestanden aan elkaar te koppelen om deze vervolgens te kunnen pseudonimiseren.

Hoewel het BSN niet bedoeld is om er wetenschappelijk onderzoek en statistiek mee te bedrijven, vormt het voorgenomen gebruik van het BSN om de verschillende bestanden aan elkaar te koppelen onzes inziens in dit geval geen probleem. Uit een onderzoek van door de rechtsvoorganger van de Autoriteit Persoonsgegevens, het College Bescherming Persoonsgegevens (CBP), blijkt dat het verbod op het gebruik van het BSN niet van toepassing is op onderzoek en statistiek, mits passende waarborgen zijn genomen.[10]

NB. Wat mogelijk wél problematisch is dat het CBP eiste dat de gegevens vóór verstrekking worden versleuteld bij de *aanbieder* van de gegevens (in casu NICE en Vektis).[11] Dat is echter in het onderhavige onderzoek niet voorzien, omdat de versleuteling pas ná verstrekking aan het CBS zal geschieden (verrinnen). **Dit vormt een juridisch risico voor dit onderzoek!**

Wij zien drie mogelijke oplossingen om dit risico te ondervangen:
1. Bij de verstrekking van het BSN wordt aangesloten bij art. 34 Wet CBS.[12] Eventueel treedt het RIVM en/of het CBS hierover met de AP in gesprek. Een positief juridisch oordeel van de AP over deze uitleg van art. 34 Wet CBS is echter niet gegarandeerd.
2. De gegevens worden door NICE, Vektis en het RIVM alsnog versleuteld alvorens de gegevens worden verstrekt aan het CBS.
3. De *koninklijke weg* is echter dat het verstrekken van de gegevens aan het RIVM en het CBS, inclusief het BSN, een wettelijke grondslag heeft als bedoeld in artikel 46 UAVG. Dit moet door VWS worden

[9] De GGD GHOR speelt, ook qua AVG, verder geen rol in dit onderzoek, maar wordt hierover wel geïnformeerd.

[10] https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/med/med_20090616_cvz.pdf.

[11] De eisen die het CBP stelde aan pseudonimisering in het algemeen waren de volgende:
- *Er wordt (vakkundig) gebruik gemaakt van pseudonimisering, waarbij de eerste encryptie plaatsvindt bij de aanbieder van de gegevens;*
- *Er zijn technische en organisatorische maatregelen genomen om herleidbaarheid van de versleuteling ("replay back") te voorkomen;*
- *De verwerkte gegevens zijn niet indirect identificerend* (NB. Deze eis is niet van belang als we aannemen dat de verrinde gegevens nog steeds persoonsgegevens zijn);
- *In een onafhankelijk deskundig oordeel (audit) wordt voor aanvang van de verwerking en daarna periodiek vastgesteld dat aan de voorwaarden 1, 2 en 3 is voldaan;*
- *De pseudonimiseringsoplossing dient op heldere en volledige wijze te zijn beschreven in een openbaar document, zodat iedere betrokkene kan nagaan welke garanties de gekozen oplossing biedt.*

[12] Art. 34 Wet CBS luidt: *De directeur-generaal (van het CBS,* PMP*) kan het burgerservicenummer opnemen in een registratie en daarvan gebruik maken ten behoeve van statistische doeleinden. De directeur-generaal kan het burgerservicenummer gebruiken in contacten met personen en instanties voor zover deze zelf gemachtigd zijn tot het gebruik van dat nummer in een registratie.*

georganiseerd, maar daar gaat tijd overheen (wetswijziging Wet publieke gezondheid, ministeriële regeling met regels voor dit onderzoek).

2 Risico's en aanbevelingen

In dit hoofdstuk vindt u een tabel met de mogelijke risico's voor de bescherming van de persoonsgegevens en de aanbevelingen daarop alsmede een overzicht van de mogelijke risico's voor betrokkenen en een advies daarop.

2.1 Mogelijke AVG risico's

In onderstaande tabel is het onderzoek opgesplitst in procesfases. Fase 1 betreft het verzamelen en aanleveren van data bij CBS; fase 2 betreft het uitvoeren van het onderzoek, fase 3 betreft het de periode van en na het afronden van het onderzoek. Per fase is aangeduid op welk onderwerpen van de AVG mogelijke risico's liggen, welke bestaande maatregelen er zijn, de overblijvende risico score en als laatst een advies hoe dit risico verlaagd kan worden tot een verwaarloosbaar risico.

Tabel 2: overzicht risico's

Fase	Mogelijke risico's voor de bescherming van de persoonsgegevens	Toelichting	Bestaande maatregelen	Risico score	Advies maatregelen
Fase 1 ***Aanleveren en verzamelen data bij CBS***	• Er meer gegevens verwerkt dan noodzakelijk (dataminimalisatie)	De onderzoeksopzet is nog niet concreet, en daardoor ook nog geen concrete afweging welke data nodig is voor dit onderzoek	Geen		Wanneer de onderzoeksvragen concreet zijn, gebruik dan alleen de data die hier expliciet voor nodig is. Schrijf ook op in het onderzoeksvoorstel voor welk doel elke data wordt gebruikt en waarom.
	• Verlies van gegevens / onbevoegde kennisneming (Informatiebeveiliging)	De gegevensoverdracht moet veilig plaatsvinden. Dit is in beginsel de verantwoordelijkheid van de verstrekker van de data. Maar als de gegevens worden geüpload in de RA-omgeving van het CBS, dan is het CBS ook verantwoordelijk voor de veilige upload van de gegevens.	(1) Beveiligde CBS data portaal voor uploaden (2) Encryptie op extra beveiligde afdeling CBS (3) VerRIN procedure CBS (pseudonimiseren) (4) Onderzoekers kunnen alleen gepseudonimiseerde gegevens inzien.		NICE heeft nog geen instellingsmachtiging voor de RA omgeving. Mocht deze worden afgewezen, dan de optie detachering bij het RIVM mogelijk verder worden uitgewerkt. Ook dit kan meegenomen worden bij de uitvoering van de DPIA na goedkeuring van het definitieve onderzoeksvoorstel. Bepaal de wijze waarop de gegevens veilig worden geüpload in de RA-omgeving. Test en train de procedure, controleer of de gegevens compleet zijn aangekomen, audit periodiek of conform de instructies wordt gewerkt.
	• Onvoldoende transparantie	Betrokkenen worden in principe niet geïnformeerd over het feit dat hun gegevens worden verstrekt ten behoeve van het onderzoek.	Geen		(1) Stel een privacyverklaring op en publiceer deze op de website van het RIVM. (2) Plaats een bericht ter kennisgeving van dit onderzoek op de website van de deelnemende partijen

	• Onvoldoende datakwaliteit	De aangeleverde gegevens moeten juist en actueel zijn	CBS levert een koppelresultaat naar de onderzoekers waaruit kan worden afgeleid wat de kwaliteit van de koppeling was.	n.v.t.	Omdat het onderzoek en statistiek betreft, raakt het in casu niet aan de bescherming van de persoonsgegevens, noch aan de risico's voor de betrokkenen.
Fase 2 ***Uitvoeren van het onderzoek***	• Ongedaanmaking van pseudonimisering	Overweging 75 AVG noemt het risico van het ongedaan maken van pseudonimisering als een risico voor de bescherming van persoonsgegevens. Omdat pseudonimisering een door art. 89 AVG aanbevolen maatregel is voor onderzoek en statistiek, is dit aspect dus cruciaal.	Het CBS heeft organisatorisch, infrastructureel en procesmatig gewaarborgd dat het omgekeerde proces de-pseudonimiseren alleen bij uitzondering en op heel gecontroleerde wijze kan plaatsvinden. Het aantal CBS medewerkers dat bevoegd is deze handeling uit te voeren is zeer beperkt (<5). Door CBS-medewerkers (RA) wordt elke output gecheckt op onthullingsrisico (minimale celvulling).		Geen
	• Personen zijn rechtstreeks identificeerbaar in de data ('*linkability* risico').	Overweging 75 AVG noemt het risico van het verlies van vertrouwelijkheid door het beroepsgeheim beschermde persoonsgegevens. Omdat de gegevens van NICE mogelijk zonder *informed consent* van de patiënt	Voor het CBS geldt op grond van art. 37 Wet CBS reeds een onthullingsverbod voor wat betreft openbaarmaking van gegevens. Ook onderzoekers van gemachtigde instellingen die werken op de RA-omgeving dienen onder toepassing van artikel 37 van de Wet CBS en dus		De personen die gaan werken met de gegevens dienen te worden gebonden aan een geheimhoudingsplicht en mogelijk ook een VOG. Dat geldt – voor zover dat nog niet reeds het geval is – ook voor personen die vanwege (technische) ondersteuning toegang hebben tot de gegevens. De gegevens moeten zodanig worden geaggregeerd dat het *linkability* risico wordt geminimaliseerd.

		gebruikt worden, is dit aspect dus cruciaal.	ook het onthullingsverbod van artikel 37 Wet CBS hun onderzoek te doen.		
	• Onvoldoende transparantie	Betrokkenen moeten in beginsel geïnformeerd worden over het gebruik van hun gegevens, tenzij het onmogelijk is of een onevenredige inspanning vergt (art. 14 AVG).	Geen		Stel een privacyverklaring op en publiceer deze op de website van het RIVM.
	• Betrokkenen kunnen hun rechten niet uitoefenen	Betrokkenen kunnen een inzage- , correctie- en/of verwijderingsverzoeken doen.	(1) Het CBS werkt vaker in dit soort opstellingen met andere partijen en heeft dan ook verschillende procedures voor de rechten van betrokkenen. (2) Pseudonimisering is technisch goed gewaarborgd door het CBS, waardoor het RIVM kan terugvallen op art. 11(1) AVG.		(1) Neem ook dit mee in de artikel 26 AVG regeling op om afspraken te maken over de gezamenlijke verwerkingsverantwoordelijkheden. (2) De verstrekker van het bronbestand kan uiteraard een verwijderings- of correctieverzoek doorvoeren. In hoeverre dit ook gevolgen heeft/moet hebben voor de onderzoeksbestanden dient nader te worden onderzocht. Een verwijderingsverzoek in de onderzoeksbestanden kan mogelijk worden geweigerd op grond van art. 17(3)(c) AVG (in hoeverre dat geldt voor de bronbestanden, is ter beoordeling van de gegevensleveranciers, en dus buiten scope van de DPIA).
	• Verlies van gegevens / onbevoegde kennisneming (Informatiebeveiliging)	Art. 89 eist passende waarborgen en art. 32 eist passende beveiligingsmaatregelen. Dit geldt niet alleen voor de RA-omgeving van het CBS, maar ook voor de wijze	De CBS omgeving is beveiligd (niet onderzocht in deze DPIA). CBS-medewerkers hebben standaard een VOG. D.m.v. rechten en doelbinding wordt alleen toegang gegeven aan data die men werkelijk nodig heeft. Ook kan er achteraf met individuele		Bepaal aan welke beveiligingsmaatregelen de onderzoekers zich moeten houden. Train de onderzoekers op de procedures. Audit periodiek of men zich aan de procedures houdt. Alleen onderzoekers kunnen op de RA omgeving werken als ze in dienst zijn bij een door de DG gemachtigde instelling.

		waarop de onderzoekers mogelijk omgaan met de gegevens buiten de RA-omgeving.	logging bekeken worden wie wanneer een bestand heeft gebruikt. Er zijn nog geen instructies voor de onderzoekers.		Onderzoekers tekenen voor geheimhouding voordat ze met microdata op de RA omgeving mogen werken.
Fase 3 ***Afronden onderzoek en bewaren gegevens***	• Gegevens worden langer bewaard dan nodig.	Gegevens mogen niet langer bewaard worden dan noodzakelijk voor het doel van de verwerking.	Binnen de RA omgeving standaard 5 jaar, na beëindiging van het project. Mocht er binnen die 5 jaar vervolgonderzoeken worden uitgevoerd, dan wordt de bewaartermijn herzien. Formeel ligt besluit bij DG van het CBS.		Bepaal wat er met de gegevens gebeurt als het onderzoek is afgelopen. Het is problematisch als het CBS brongegevens bewaart die het niet op basis van haar CBS taak heeft verkregen. De bevoegdheid om te besluiten over dergelijke gegevens ligt bij het RIVM. Maak hierover afspraken in de art. 26 regeling.
	• Verlies van gegevens / onbevoegde kennisneming (Informatiebeveiliging)	De gegevens moeten op een veilige manier worden verwijderd (art. 32 AVG).	De procedure bij het CBS is ons onbekend		Maak hierover afspraken in de art. 26 regeling.

Legenda:

= Verwaarloosbaar/Niet van toepassing

= Gering (kleine kans op negatieve gevolgen en/of eventuele gevolgen zijn waarschijnlijk herstelbaar)

= Substantieel (significante kans op negatieve gevolgen en/of eventuele gevolgen zijn waarschijnlijk onherstelbaar)

= Kritiek (de kans op negatieve gevolgen is groot en eventuele gevolgen zijn waarschijnlijk onherstelbaar)

De overige in overweging 75 genoemde risico's achten wij niet relevant.

2.2 Risico's voor betrokkenen

Binnen de scope van het onderzoek en de waarborgen van artikel 89 worden gehanteerd (zie hoofdstuk 1, paragraaf 1.4) en de onomkeerbare pseudonimisering van het onderzoek, is er vanwege het statistische karakter van het onderzoek in principe geen risico voor de betrokkenen.

Bij de-pseudonimisering en een mogelijk datalek zou dit op verschillende vlakken wel impact kunnen hebben op de burger. De kans dat dit gebeurt is in deze fase van de onderzoeksopzet nog niet volledig in te schatten. Daarom wordt in dit overzicht alleen gekeken naar de mogelijke impact die het zou hebben, mocht een gede-pseudonimiseerd datalek voorkomen. In tabel 3 Risico's voor betrokkenen worden deze verder toegelicht.

Vanwege de gevoelige en bijzondere data die wordt gebruikt in dit onderzoek, raden wij aan om een uitgebreide DPIA uit te voeren en deze jaarlijks te herzien.

Tabel 3: Risico's voor betrokkenen

Aard van het risico	Impact	Score	Opmerkingen / advies
Risico voor de veiligheid van de betrokkenen en/of zijn familie	Verwaarloosbaar		Het CBS heeft conform wettelijke eisen m.b.t. privacy en de AVG een proces ingericht om persoonsgevoelige gegevens te pseudonimiseren (verrinnen). Het CBS heeft organisatorisch, infrastructureel en procesmatig gewaarborgd dat het omgekeerde proces de-pseudonimiseren alleen bij uitzondering en op heel gecontroleerde wijze kan plaatsvinden. Het aantal CBS medewerkers dat bevoegd is deze handeling uit te voeren is zeer beperkt (<5).
Risico op inbreuk op de persoonlijke levenssfeer	Substantieel (inbreuk op medisch beroepsgeheim)		Het CBS heeft conform wettelijke eisen m.b.t. privacy en de AVG een proces ingericht om persoonsgevoelige gegevens te pseudonimiseren (verrinnen). Het CBS heeft organisatorisch, infrastructureel en procesmatig gewaarborgd dat het omgekeerde proces de-pseudonimiseren alleen bij uitzondering en op heel gecontroleerde wijze kan plaatsvinden. Het aantal CBS medewerkers dat bevoegd is deze handeling uit te voeren is zeer beperkt (<5).
Risico op inbreuk op de bescherming van de lichamelijke integriteit	Geen		
Risico op onrechtvaardige behandeling	Verwaarloosbaar		
Risico op discriminatie	Verwaarloosbaar		Het onderzoek richt zich niet op individuen. Echter, als de gegevens in herleidbare vorm zouden lekken of in strijd met de procedures van het CBS openbaar worden gemaakt, dan staat dit risico op rood.
Risico op beschadiging van reputatie	Verwaarloosbaar (medische risicogroepen)		Het onderzoek richt zich niet op individuen. Echter, als de gegevens in herleidbare vorm zouden lekken of in strijd met de procedures van het CBS openbaar worden gemaakt, dan staat dit risico op rood.
Risico op aantasting van de autonomie / zelfbeschikking	Gering		Betrokkenen kunnen niet kiezen of hun gegevens in het onderzoek worden betrokken. De uitzondering op de hoofdregel dat toestemming nodig is, dient derhalve goed te worden onderbouwd in het onderzoeksvoorstel en in de privacyverklaring.

Risico op aantasting menselijke waardigheid	Verwaarloosbaar		
Risico's voor bescherming overige (grond)rechten	Verwaarloosbaar		
Risico op aanzienlijk economisch of maatschappelijk nadeel	Verwaarloosbaar		Het onderzoek richt zich niet op individuen. Echter, als de gegevens in herleidbare vorm zouden lekken, dan staat dit risico op oranje.

Legenda:

= Verwaarloosbaar/Niet van toepassing

= Gering (kleine kans op negatieve gevolgen en/of eventuele gevolgen zijn waarschijnlijk herstelbaar)

= Substantieel (significante kans op negatieve gevolgen en/of eventuele gevolgen zijn waarschijnlijk onherstelbaar)

= Kritiek (de kans op negatieve gevolgen is groot en eventuele gevolgen zijn waarschijnlijk onherstelbaar)


PRIVACY
MANAGEMENT
PARTNERS

Privacy
Management
Partners
Coöperatie UA

adres
Vondellaan 58
3521 GH Utrecht

telefoon
+31 85 401 38 66

e-mail
info@pmpartners.nl

website
www.pmpartners.nl