# Gegevensbeschermings-effectbeoordeling (PIA)

**Ministerie van VWS**

**Publieke gezondheid/Programmadirectie COVID 19**

Den Haag 2 oktober 2020

Vaststelling verwerkersverantwoordelijke: 10 oktober 2020
Naam: [redacted]

Advies [redacted] 2 november 2020
Naam: [redacted]

Advies [redacted] 2 november 2020
Naam: [redacted]

# Gegevensbeschermings-effectbeoordeling (PIA)

**Ministerie van VWS**

**Publieke gezondheid/Programmadirectie COVID 19**

**Contact:**

Ministerie VWS, Directie Publieke Gezondheid/Programmadirectie COVID 19

5.1.2e 5.1.2e

5.1.2e @minvws.nl

5.1.2e

Versie: 3.0, 27 oktober 2020

# Inhoudsopgave

# Inleiding

Voeg hier wanneer gewenst een openingsalinea of inleiding toe. Denk bijvoorbeeld aan:
- Verwijzing naar het privacybeleid of motivatie achter de uitvoering van deze PIA
- Informatie over de manier van opstellen.

# 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.**

Tijdens de eerste COVID-19 golf in maart/april werden voornamelijk die mensen getest die in het ziekenhuis terecht kwamen waardoor de gegevens in het meldsysteem van de GGD'en aan het RIVM (Osiris) vrij accuraat waren. GGD'en zijn op basis van de Wpg wel verplicht om een besmetting via Osiris door te geven, maar niet om een opname door te geven. Nu de testen meer los staan van de opname betekent dit dat het Osiris-systeem niet meer toereikend is om een goed beeld te hebben van de ziekenhuisopnamen als gevolg van de epidemie.

De gegevens van NICE zijn in dit kader een stuk accurater. Om die reden wil het Corona dashboard deze gegevens gebruiken. Daarbij is het noodzakelijk dat op gemeenteniveau duidelijk wordt hoeveel mensen in het ziekenhuis liggen. Dit cijfer samen met de positieve testen in de gemeente geven de burgemeester en de voorzitter van de veiligheidsregio een completer beeld om de situatie te bezien en de goede maatregelen te nemen. Echter, de NICE-gegevens bevatten geen gemeentecode.

Vanwege de betere kwaliteit en de volledigheid wil het RIVM voor de modellering ook overgaan op het gebruik van de gegevens van NICE. Daarvoor is het noodzakelijk dat ook het geslacht van de mensen die opgenomen zijn in het ziekenhuis wordt gebruikt omdat de intensiteit van het verloop van de ziekte voor mannen en vrouwen verschillend is. In de NICE-gegevens is echter ook geen geslachtsaanduiding beschikbaar.

Verrijking van de gegevens van NICE met gemeentecode en geslachtsaanduiding kan via een koppeling met de Basisregistratie Persoonsgegevens via het BSN. Voor deze koppeling is deze gegevensbeschermingseffecbeoordeling bedoeld.

## 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.**

Voor de overgang van Osiris naar NICE moet gemeentecode en geslachtsaanduiding bekend zijn. Deze kan slechts verkregen worden via koppeling van de NICE-data middels BSN aan de BRP. Daarvoor worden dus BSN en gegevens omtrent de gezondheid van personen verwerkt. Dit betreft mensen waarvan, via de NICE-registratie is vastgesteld dat ze op de IC of op een verpleegafdeling van een ziekenhuis zijn opgenomen. NICE stelt de volgende gegevens uit de NICE-registratie beschikbaar voor het RIVM:

- Patient-id (Pid)
- Seq: hoeveelste record per patiënt
- Naam ziekenhuis
- Leeftijd
- Opnamedatum
- Ontslagdatum
- Reden van ontslag (alleen bij IC-opnames: bijv. overlijden, verpleegafdeling, ander ziekenhuis, naar huis)
- Komt patiënt van een andere IC: j/n (alleen bij IC-opnames)
- (Overgeplaatst naar) naam ziekenhuis (alleen bij IC-opnames)
- Betreft dit een IC-opname: j/n
- Overleden bij ontslag (j/n)
- Covid19-status: bijv. lab, ct, verdacht

Het Patiënt-id (Pid) is een pseudoniem dat door KIK/AMC wordt aangemaakt en alleen binnen de NICE-registratie betekenis heeft. Het heeft geen relatie met nummers of sleutels die in de ziekenhuizen gebruikt worden.
Verderop in dit document is sprake van drie bestanden van NICE die beschikbaar zijn voor het RIVM. De drie bestanden bevatten bovenstaande gegevens of een selectie hiervan. Er zijn geen andere gegevens beschikbaar voor het RIVM.

## 3. Gegevensverwerkingen

**Geef alle voorgenomen gegevensverwerkingen weer.**

De Stichting NICE is een stichting zonder winstoogmerk en is opgericht door de beroepsgroep van intensivisten voor intensivisten. Inmiddels doen alle Nederlandse IC's mee aan dit initiatief en worden per jaar de gegevens van ongeveer 80.000 nieuwe IC opnamen aan de NICE database toegevoegd. De afdeling klinische informatiekunde (Medical Informedics) van het AMC (KIK/AMC) verwerkt voor alle ziekenhuizen de gegevens voor de Stichting NICE. Deze verwerking valt buiten de verwerking waar deze PIA op ziet aangezien de ziekenhuizen verwerkingsverantwoordelijk zijn voor deze verwerking. KIK/AMC is verwerker. De Stichting NICE heeft het mandaat van de ziekenhuizen om als verwerkingsverantwoordelijke op te treden en KIK/AMC als verwerker aan te sturen.

Gegevensverwerking:
Om de datastromen inzichtelijk te maken is als bijlage (PIA stroomschema dataverwerking.docx) een stroomschema bijgevoegd. Hieronder wordt tekstueel verwoord wat in de bijlage te zien is.

- Het RIVM heeft momenteel toegang tot een besloten, beveiligde omgeving van stichting NICE, waaruit zij een drietal speciaal voorbereide bestanden kunnen betrekken ('pullen') (stroom 1). In de registratie van NICE wordt aan elk record met hetzelfde BSN een Pid (persoonlijk identificatienummer) toegevoegd. Dit is een door NICE gegenereerd nummer voor intern gebruik. Deze Pid komt ook mee in één van de bestanden die klaargezet worden voor het RIVM. In geen van deze drie bestanden wordt BSN meegeleverd.
- Om gemeentecode en geslachtsaanduiding toe te voegen aan de gegevens, is het wel nodig dat BSN meegeleverd wordt. Voor het verkrijgen van de gemeentecode, de leeftijd en het geslacht uit de BRP wordt straks, naast de drie hierboven genoemde bestanden, een apart koppelbestand met alleen BSN en Pid gemaakt. Dit wordt door NICE in een aparte beveiligde omgeving beschikbaar gesteld (stroom 2). Middels BSN wordt door een geautoriseerde datamanager van het RIVM een automatische koppeling gemaakt met de BRP en wordt gemeentecode en geslacht toegevoegd (stroom 3). Vervolgens wordt het BSN verwijderd. De tabel met Pid, gemeentecode en geslacht wordt daarna automatisch via het Pid gekoppeld aan de andere bestanden (stroom 4). Deze bestanden worden dan beschikbaar gesteld aan de RIVM-onderzoekers (stroom 5). Onderzoekers van RIVM hebben zelf op geen enkel moment toegang tot BSN.
- Onderzoekers van het RIVM genereren dagelijks een geaggregeerd bestand met aantallen opgenomen patiënten per gemeente ten behoeve van het coronadashboard (stroom 6). Daarnaast genereren ze wekelijks een tabel met het landelijk aantal ziekenhuisopnamen de afgelopen week, uitgesplitst naar leeftijd en geslacht ten behoeve van het epidemiologisch rapport. Dat is zodanig geaggregeerd dat op geen enkele wijze meer sprake is van herleidbaarheid. Ten slotte worden de ziekenhuisopnamen en leeftijd en geslacht gebruikt als input voor modelleerwerk, onder andere voor de bepaling van het Reproductiegetal en het aantal besmettelijken. Alleen de output (reproductiegetal en aantal besmettelijken) wordt gepubliceerd.
- De anonieme data, namelijk patiënten in het ziekenhuis per gemeentecode worden op het dashboard geplaatst.

## 4. Verwerkingsdoeleinden

**Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.**

Het doel van de verwerking van het BSN en de gegevens omtrent de gezondheid is het bieden van inzicht aan de burgemeesters en voorzitters van de veiligheidsregio's in de ziekenhuisopnames uit hun regio.
Het dashboard wil de gegevens van NICE graag uitsplitsen naar regio en gemeente. Dit is noodzakelijk omdat de aanpak van de crisis gedeeltelijk op regionaal niveau moet plaatsvinden. Het is van belang dat de voorzitters van de veiligheidsregio een accuraat beeld hebben van de situatie in hun regio. Veiligheidsregio's en burgemeesters hebben de behoefte om te weten hoeveel van de mensen uit hun regio respectievelijk gemeente in een ziekenhuis liggen, ongeacht waar dat ziekenhuis staat. Alleen positieve tests zijn niet voldoende. Ziekenhuisopnamen geven als toegevoegde waarde een beeld van de ernst van de infecties. Alleen de aantallen positieve tests geven dat beeld niet. Een hoog percentage in het ziekenhuis opgenomen mensen geeft een hogere urgentie dan een laag percentage, ongeacht het aantal besmettingen.
De aanpak van het virus vindt plaats op zowel het landelijke als het regionale niveau. Het merendeel van de maatregelen is landelijk, maar op regionaal niveau kunnen deze maatregelen door de voorzitter van de veiligheidsregio dan wel de burgemeester worden aangevuld als blijkt dat er in die regio/gemeente aanvullende maatregelen moeten worden genomen. Dit was bijvoorbeeld het geval bij de verplichting tot het dragen van mondkapjes in drukke winkelstraten die door meerdere burgemeesters werd afgekondigd. Om een goede inschatting te kunnen maken of er aanvullende maatregelen nodig zijn, moet de burgemeester inzicht hebben in de actuele data over het aantal positieve testen als ook de aantallen mensen die in het ziekenhuis liggen.
Het doel van het verwerken van de gegevens geslacht en geboortejaar is het verbeteren van de modellen die gebruikt worden bij het RIVM. Belangrijk output uit deze modellen zijn het reproductiegetal en het aantal besmettelijken. Het geslacht en geboortejaar van de opgenomen persoon zijn van belang voor de duiding van de hevigheid van de infectie en zijn nodig voor het modelleren.

## 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.**

De afdeling klinische informatiekunde (Medical Informedics) van het AMC (KIK/AMC) verzamelt voor de Stichting NICE gegevens over ziekenhuis- en IC-opnamen als gevolg van COVID-19 op basis van een overeenkomst tussen NICE en de ziekenhuizen. AMC/KIK is verwerker. De ziekenhuizen zijn verwerkingsverantwoordelijk. De Stichting NICE heeft het mandaat van de ziekenhuizen om als verwerkingsverantwoordelijke op te treden en KIK/AMC als verwerker aan te sturen.
Er bestaat een overeenkomst tussen het RIVM en KIK/AMC over het "pullen" van gegevens door het RIVM.

Het RIVM betrekt de gegevens uit het systeem van KIK/AMC. Het RIVM refereert de gegevens met de BRP middels een koppeltabel met een uniek Pid en het BSN om de gemeentecode en het geslacht te verkrijgen. Voor deze verwerking is het RIVM verwerkingsverantwoordelijk in de zin van de AVG. De combinatie geslacht, geboortejaar en het gegeven dat iemand opgenomen is, wordt gebruikt ten behoeve van modellering. De geaggregeerde aantallen per gemeentecode worden door het RIVM doorgegeven aan het corona dashboard.

VWS beheert het corona dashboard. De gegevens die op het dashboard geplaatst worden zijn anonieme gegevens. De landelijke gegevens van stichting NICE is open data. De regionale gegevens worden straks ook als open data gepubliceerd.

## 6. Belangen bij de gegevensverwerking

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

Stichting NICE registreert alle IC-opnamen in Nederland alsmede de opnamen op een verpleegafdeling als gevolg van COVID. De registratie van IC-opnamen door NICE is hun corebusiness. In het voorjaar van 2020 heeft NICE van het Ministerie van VWS het verzoek gekregen om ook de opnamen op een verpleegafdeling als gevolg van COVID te gaan registreren.

Het RIVM is het nationale centrum voor de bestrijding van infectieziekten. RIVM is verwerkingsverantwoordelijk. RIVM heeft toegang tot een besloten omgeving van NICE waaruit ze de ziekenhuisopnamen betrekt. Ook heeft RIVM toegang tot een webservice van T&T waarmee via BSN een koppeling gemaakt kan worden om gemeentecode te verkrijgen.
RIVM publiceert aantal ziekenhuisopnamen per gemeente als open data op https://data.rivm.nl/covid-19

VWS maakt het Corona Dashboard en publiceert aantal ziekenhuisopnamen per Veiligheidsregio en gemeente.

## 7. Verwerkingslocaties

**Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.**

De gegevensverwerking zal alleen in Nederland dan wel de EU plaatsvinden

## 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.**

Verwerking van de datastromen wordt geautomatiseerd. Meer detail over de datastromen is te vinden onder *3. Gegevensverwerkingen* en in de bijlage: PIA stroomschema dataverwerking.docx. Er is hier geen sprake van besluitvorming, alleen van dataverwerking. Het systeem is zodanig ingericht dat inhoudelijke data en het BSN nooit in één bestand bij elkaar staan.

De datamanager van het RIVM heeft toegang tot een beveiligde omgeving van NICE. Daarin zijn in twee aparte omgevingen in totaal vier datasets voor het RIVM klaargezet. De connectie tussen RIVM en NICE wordt gelegd via een lijnencryptie. De data wordt versleuteld zodat deze beveiligd overgedragen wordt. De geautoriseerde datamanager voor de beveiligde omgeving moet inloggen met een gebruikersnaam en een wachtwoord.

In de ene omgeving is een koppelbestand met BSN en Pid beschikbaar gesteld. Dat is het enige bestand waarin BSN beschikbaar is. Koppeling van BSN aan gemeentecode en geslacht gaat via een real time XML-webservice. Een lijst van BSN-nummers en een Pid (intern persoonlijk identificatienummer) wordt aangeboden via deze webservice aan een Trusted Third Party (T&T). Vrijwel real-time komt een antwoord terug met toevoeging van *Gemeente van inschrijving* (Gemeentecode) en *geslacht* via koppeling aan het BSN. BSN wordt vervolgens (eveneens geautomatiseerd) verwijderd.
(Zie ook bijlage: XML-koppeling webservice GBA-V adhoc.pdf)

De datamanager heeft ook toegang tot de andere omgeving waarin de andere drie bestanden beschikbaar zijn. Deze bestanden worden daar, eveneens geautomatiseerd, uit betrokken. Vervolgens wordt aan één van deze bestanden, via de Pid, de gemeentecode en de geslachtsaanduiding gekoppeld.

De geautomatiseerde procedure wordt zodanig ingericht dat BSN en inhoudelijke data nooit tegelijkertijd in dezelfde omgeving beschikbaar is.

## 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.**

Op deze verwerking zijn naast de AVG, de wet op het RIVM en de Wet burgerregistratie personen (Wet BRP) van toepassing. De Wet op het RIVM is van toepassing omdat deze wet de taken en bevoegdheden van het RIVM vastlegt. De Wet BRP is van toepassing omdat inzage in de BRP moet voldoen aan de vereisten van de Wet BRP en er een autorisatiebesluit nodig is vanuit de Wet BRP. Het RIVM is in bezit van meerder autorisatiebesluiten.
Het autorisatiebesluit dat voor deze verwerking van persoonsgegevens van toepassing is, is het besluit van 30 juli 2014: 2014-0000415392 (zie bijlage: Bijlage - stcrt-2014-26825.pdf). Dit besluit heeft betrekking op het doen van onderzoek door het RIVM. Voor de definitie van onderzoek wordt in het autorisatiebesluit verwezen naar artikel 3 van de wet op het RIVM. Onderzoek in het eerste lid onder a van artikel 3 van de wet op het RIVM ziet niet op preventieprogramma's zoals de bevolkingsonderzoeken, maar op andersoortig onderzoek. Het onderzoek moet gericht zijn op de ondersteuning van beleidsontwikkeling, de beleidsuitvoering, de bewaking van de veiligheid en de uitoefening van toezicht op het gebied van de volksgezondheid en het milieu.
Het onderzoek dat het RIVM in dit kader doet is gericht op onderzoek voor de praktijk, op de ondersteuning van de beleidsontwikkeling en tevens op de uitoefening van toezicht op het gebied van de volksgezondheid. Het RIVM speelt een centrale rol bij bestrijding van infectieziekten en de bestrijding van het COVID-19 virus gedurende deze crisis. Het RIVM geeft aan dat dat de mensen die in het ziekenhuis liggen deelnemers zijn aan het onderzoek naar de regionale spreiding van corona en het onderzoek naar de modellering van de virusuitbraak.

## 10. Bewaartermijnen

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

De gegevens op het dashboard zijn in beginsel anonieme gegevens. RIVM heeft BSN alleen nodig voor koppeling met BRP. Zodra koppeling is gemaakt, gemeentecode en geslacht is geretourneerd, worden de BSN-nummers verwijderd. Dit gebeurt middels een geautomatiseerd proces. Koppeling met de andere gegevens uit de NICE-registratie gaat dan via het persoonlijk identificatienummer dat alleen binnen NICE waarde heeft. Het gaat hier om de volgende attributen:

- Patient-id
- Seq: hoeveelste record per patiënt
- Naam ziekenhuis
- Leeftijd
- Opnamedatum
- Ontslagdatum
- Reden van ontslag (alleen bij IC-opnames: bijv. overlijden, verpleegafdeling, ander ziekenhuis, naar huis)
- Komt patiënt van een andere IC: j/n (alleen bij IC-opnames)
- (Overgeplaatst naar) naam ziekenhuis (alleen bij IC-opnames)
- Betreft dit een IC-opname: j/n
- Overleden bij ontslag (j/n)
- Covid19-status: bijv. lab, ct., verdacht

Elk uur zet Stichting NICE geactualiseerde bestanden klaar. Het oude bestanden worden verwijderd.

Voor het (periodiek) verzamelen en verwerken van medische gegevens is er een wettelijke bewaartermijn van 15 jaar na onderzoek. Corona is echter door het Nationaal Archief aangewezen als zogenaamd hotspotdossier. Dit betekent dat alle documenten permanent bewaard moeten worden. VWS, RIVM en het Nationaal Archief zijn momenteel echter in gesprek over databestanden met herleidbare persoonsgegevens. Het RIVM staat op het standpunt dat documenten met herleidbare persoonsgegevens niet onder de hotspot zouden moeten vallen, dus deze zouden de bewaartermijn van 15 jaar houden. De documenten waarin de persoonsgegevens niet herleidbaar zijn, vallen wel onder de hotspot en moeten dus voor altijd bewaard blijven. De bewaartermijn is dus afhankelijk van de soort informatie.

# 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.**

Ten aanzien van het BSN, geslacht en leeftijd geldt voor het RIVM dat zij – in overeenstemming met artikel 10 Wet BSN - dit verwerken ten behoeve van de uitvoering van hun taak van algemeen belang in de zin van artikel 6, eerste lid onder e AVG. Het RIVM heeft immers als taak om de ontwikkelingen op het terrein van de volksgezondheid te onderzoeken en monitoren zoals neergelegd is in artikel 3, eerste lid onder a en onder e van de Wet op het RIVM juncto artikel 6c Wet publieke gezondheid.

## 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.**

De verwerking betreft twee verschillende verwerkingen die aan elkaar gerelateerd zijn en deels overlappen.

**Uitsplitsen ten behoeve van het hebben van regionale gegevens op het coronadashboard.**
Hiervoor worden bijzondere persoonsgegevens verwerkt. De grondslag voor deze verwerking persoonsgegevens kan gevonden worden in artikel 9, tweede lid onder g van de AVG. Dit betreft de grond noodzakelijk voor redenen van zwaarwegend algemeen belang dat is neergelegd in lidstatelijk recht. De noodzaak is erin gelegen dat een deel van de crisis op regionaal niveau moet worden aangepakt. Burgemeesters en voorzitters van veiligheidsregio's hebben hiervoor de gegevens nodig omtrent het aantal positieve testen en de aantallen mensen die in het ziekenhuis liggen. Artikel 9, tweede lid onder g vereist als basis lidstatelijk recht. Dit kan gevonden worden in artikel 3, eerste lid onder a en e en het derde lid van de wet op het RIVM alsmede in artikel 6c Wet publieke gezondheid.

**Verbeteren van de modellering van het RIVM**
Ten behoeve van de verbetering van de modellering van het RIVM worden bijzondere persoonsgegevens verwerkt. Dit betreffen gegevens omtrent de gezondheid, zoals onder *2. Persoonsgegevens* benoemd. De grondslag voor het verwerken van deze gegevens kan gevonden worden in artikel 9, tweede lid onder g van de AVG. De verwerking is noodzakelijk voor redenen van zwaarwegend algemeen belang. De modellering is noodzakelijk om goed te kunnen voorspellen hoe de besmettingen en de ziekenhuisbezetting zal verlopen. Het is bekend dat het geslacht en tevens de leeftijd van een persoon van invloed zijn op de intensiteit van de ziekte en op de duur van een ziekenhuisopname. Daarom is het noodzakelijk dat deze gegevens worden verwerkt ten behoeve van de modellering. Artikel 9, tweede lid onder g vereist een basis in lidstatelijk recht. Deze basis kan gevonden worden in artikel 3, eerste lid onder a en e jo. het derde lid van artikel 3 van de Wet op het RIVM, alsmede in artikel 6c Wet publieke gezondheid.

Het RIVM heeft een wettelijke grondslag om BSN te verwerken.

## 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.**

Het doel van deze verwerking is tweeledig:

1. Op regionaal niveau inzichtelijk maken voor de burgemeesters en voorzitters van de veiligheidsregio's hoeveel mensen er uit een bepaalde regio/gemeente in het ziekenhuis liggen met COVID-19. Deze gegevens geeft de burgemeester en de voorzitter inzicht, in aanvulling op het aantal positieve testen, om te zien of het noodzakelijk is om aanvullende maatregelen te nemen.
2. Toevoeging van het persoonsgegeven geslachtsaanduiding aan de registratie zodat de registratie geschikt wordt als basis voor de modellering van de Corona-pandemie door het RIVM. Samen met de leeftijd is het geslacht belangrijk in de modellering. Hierdoor kan het Reproductiegetal en het aantal besmettelijken accurater worden gemodelleerd. Deze modellen spelen een belangrijke rol bij de opschaling en afschaling van Corona-maatregelen in de samenleving.

## 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?.**

Het doel van het dashboard is om zicht en grip op het virus te houden, zoals dat onder meer verwoord is in de Kamerbrieven van 16 juli 2020 en 1 september 2020 (Respectievelijk: 'Lessen verpleeghuizen met het oog op een eventuele tweede golf' en 'Lessons learned COVID-19').

Data over dagelijkse ziekenhuisopnames op gemeenteniveau zijn momenteel nog afkomstig van RIVM (Osiris). Osiris geeft echter een onderschatting. Registratie is niet verplicht en daardoor niet compleet. Voor het dashboard willen we daarom overstappen op gegevens van Stichting NICE. Stichting NICE geeft een veel beter beeld van de dagelijkse instroom van het aantal patiënten op de IC en op de verpleegafdelingen van de ziekenhuizen.
Echter, NICE heeft de uitsplitsing van het aantal patiënten naar gemeente niet standaard beschikbaar. Daarvoor moet een koppeling gemaakt worden via het BSN met de Basisregistratie Persoonsgegevens (BRP). Grondslag hiervoor moet gevonden worden in de noodzaak voor de beschikbaarheid van deze cijfers op gemeenteniveau.

Het aantal ziekenhuisopnamen per 100.000 inwoners is op gemeenteniveau een belangrijke medische indicator. Dit geeft lokale stuurinformatie voor de gemeenten en de Veiligheidsregio's, die oa. gebruikt wordt in het wekelijkse inschalingsoverleg en om te bepalen of er (aanvullende) lokale maatregelen nodig zijn per gemeente of veiligheidsregio. Naast ziekenhuisopnamen zijn hiervoor op gemeenteniveau ook meldingen van positieve tests van besmette patiënten bekend. Deze gegevens geven een eerder beeld over de verspreiding van het virus, maar zijn minder volledig. Positieve testcijfers zijn namelijk afhankelijk van testbereidheid en beschikbaarheid van tests. Naar schatting laat 20% à 30% van de Nederlanders zich testen. Op gemeenteniveau geven ziekenhuisopnamen samen met positieve tests zicht en grip op de spreiding van het virus; beide indicatoren vullen elkaar aan. Het aantal ziekenhuisopnames is de enige indicator die laat zien welke ernstige gezondheidseffecten het virus in een gemeente of regio heeft. Het is daarom een essentiële indicator voor burgemeesters om mee te sturen, en voor het kabinet om te zien in welke gemeentes en regio's de ernst van de verspreiding van het virus het grootst is. Hierdoor kan accurater en eerder worden ingegrepen, waardoor het virus beter onder controle blijft.

Daarnaast wordt de informatie gebruikt door burgers om de situatie in de eigen woonplaats te kunnen volgen en om zelf geïnformeerd risico- afwegingen te maken. Door deze informatie gecentraliseerd als open data beschikbaar te stellen wordt het principe van data-minimalisatie gerespecteerd: In plaats dat gemeentes zelf informatie op BSN gaan koppelen, wordt dit veilig centraal gedaan door het RIVM dat in een fase 1 pandemie de bevoegdheid heeft om landelijk beleid uit te voeren, en hier persoonsgegevens voor te verwerken.

**Proportionaliteit**
De verwerking kan als proportioneel worden aangemerkt omdat inmenging in de persoonlijke levenssfeer zeer beperkt is. Deze staat in verhouding tot het doel zijnde de verbetering van monitoring en modellering van de pandemie in Nederland. Wanneer het BSN naast de BRP wordt gelegd, worden alleen de gemeentecode en het geslacht opgevraagd. Verdere informatie uit de BRP wordt niet verwerkt en kan ook niet worden ingezien.

**Subsidiariteit**
Vanuit het oogpunt van subsidiariteit is er gekeken of het doel ook bereikt kan worden met gebruik van een ander middel, dan wel door gebruik van minder vergaande maatregelen.
Het enige alternatief voor de koppeling met het BRP zou zijn dat aan de NICE-registratie vanuit de ziekenhuizen, eventueel via de postcode, een gemeentecode wordt toegevoegd. We hebben hier echter te maken met een lopende registratie. Daardoor zou met terugwerkende kracht via de EPD's in de ziekenhuizen aan alle ziekenhuisopnamen een gemeentecode moeten worden toegevoegd. Dit is een zeer tijdrovend traject dat, gezien de urgentie van de monitoring van de pandemie feitelijk alleen een theoretisch alternatief is.

Alternatief zou ook kunnen zijn dat NICE het eerste ziekenhuis registreert waar iemand binnen is gekomen. Dit is geen optie omdat dit ook handmatig registreren tot resultaat zou hebben. Daarbij komt dat een ziekenhuis vaak mensen uit meer dan één veiligheidsregio opvangt waardoor de gegevens niet bijdragen aan het uitgezette doel.
NICE mag niet zelf de koppeling met de BRP maken, omdat het daarvoor niet gerechtigd is.
Andere alternatieven zijn niet beschikbaar.

## 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.**

Er is voor gekozen om de rechten van betrokkene te beperken. Het is noodzakelijk dat de gegevens volledig zijn en er is slechts voor een korte periode sprake van persoonsgegevens.

Doel 1: Uitsplitsen gegevens naar gemeente
De gegevens zijn slechts een korte periode herleidbare persoonsgegevens. Zodra de gemeentecode en de geslachtsaanduiding is gekoppeld bij de BRP, wordt het BSN gewist. Vervolgens worden gemeentecode en geslachtaanduiding via het Pid gekoppeld aan de overige data. Ten behoeve van het dashboard vind een aggregatie naar gemeente plaats. Dan blijven alleen de aantallen per gemeente over. Op dat moment kan er gesproken worden over anonieme data.

Vanaf het moment dat er sprake is van anonieme data is deze niet meer te herleiden. Conform artikel 11 AVG moet de verwerkingsverantwoordelijke de betrokkene bij aanvraag erop wijzen dat de gegevens niet meer te herleiden zijn, maar zijn verder de bepalingen van artikel 15 t/m 20 AVG niet van toepassing.

Echter voor een zeer korte periode zijn de gegevens wel herleidbaar. In dit geval is het belangrijk dat betrokkene niet de mogelijkheid heeft om zijn gegevens te wissen. In dit kader worden de rechten van betrokkene beperkt conform artikel 17, derde lid onder b waarin is geregeld dat in het recht op wissing van gegevens niet van toepassing is in het geval de verwerking geschiedt voor de uitvoering van een taak van algemeen belang. Het is voor de uitvoering van de taak van belang dat de gegevens niet aangetast worden.

Doel 2: Modellering
De gegevens zijn slechts een korte periode persoonsgegevens. Zodra de gegevens zijn ontvangen worden deze op basis van BSN gematcht aan de BRP voor de gemeentecode en het geslacht wordt BSN verwijderd. De Pid wordt gebruikt voor koppeling aan de gezondheid gerelateerde gegevens. De gegevens zijn niet meer direct te herleiden. Conform artikel 11 AVG moet de verwerkingsverantwoordelijke de betrokkene bij aanvraag erop wijzen dat de gegevens niet meer te herleiden zijn. De bepalingen van artikel 15 t/m 20 AVG zijn daarom niet van toepassing op deze data.
Echter, voor een korte periode zijn de gegevens wel herleidbaar. In dit geval is het belangrijk dat betrokkene niet de mogelijkheid heeft om zijn gegevens te wissen. In dit kader worden de rechten van betrokkene beperkt conform artikel 17, derde lid onder b waarin is geregeld dat in het recht op wissing van gegevens niet van toepassing is in het geval de verwerking geschiedt voor de uitvoering van een taak van algemeen belang. Het is voor de uitvoering van de taak van belang dat de gegevens niet aangetast worden.

# 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:**

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

1. KIK/AMC verwerkt BSN zonder wettelijke grondslag
   A. RIVM krijgt een lijst met BSN's waarvoor het onduidelijk is of de partij die de lijst deelt een wettelijke grondslag heeft.
   B. Goedkeuring voor het verzamelen van BSN door NICE is verleend middels een brief van VWS aan de ziekenhuizen. Dit is geen wettelijke grondslag.
   C. Waarschijnlijkheid is groot.
   D. Gevolgen voor de betrokkenen zullen nihil zijn. Gedurende het proces van dataverrijking wordt BSN zo snel mogelijk verwijderd waardoor de gegevens niet meer direct herleidbaar zijn. Gegevens worden vervolgens alleen voor statistische doeleinden gebruikt.

2. Foutief BSN wordt geregistreerd
   A. Dit kan ertoe resulteren dat de persoonsgegevens van mensen die niet in het ziekenhuis liggen, geregistreerd worden. De gegevens worden voor geen ander doel gebruikt.
   B. Foutieve registratie bij NICE of ziekenhuis
   C. Ligt aan het systeem. Bij handmatige invoering is deze kans groot. Bij automatische gegevensdeling is dit beperkt.
   D. De impact voor de betrokkene is nihil. Er hangen geen gevolgen aan voor betrokkene. Het gebruik van de data is slechts voor statistische doeleinden.

3. Gegevens worden langer bewaard dan noodzakelijk
   A. Individuele gegevens kunnen langer dan afgesproken worden gekoppeld aan bronnen met andere individuele gegevens
   B. Koppeling en vervolgens verwijdering van BSN wordt geautomatiseerd. Scripts kunnen stuklopen nadat koppeling is gedaan, maar voordat BSN is verwijderd.
   C. Kleine kans dat het script juist tussen deze twee acties breekt. Of het hele script start niet (en er is dus ook geen koppeling geweest) of het hele script wordt uitgevoerd en BSN's worden verwijderd. In geval het script niet werkt en BSN's dus niet verwijderd worden, wordt dat onmiddellijk opgemerkt omdat noodzakelijke data ontbreekt en zal het script opnieuw gestart worden.
   D. Impact voor betrokkene is nihil. BSN's zijn niet elders beschikbaar

4. Er is sprake van een datalek
   A. De combinatie van BSN en het feit dat de persoon met deze BSN opgenomen is in een ziekenhuis is bekend.
   B. Beveiligingslek in koppeling RIVM en Trusted Third Party (T&T) of beveiligingslek tussen KIK/AMC en RIVM.
   C. T&T: Kans is zeer klein. RIVM werkt als jaren samen met T&T. T&T staat bekend als zeer beetrouwbare partij die volledig gespecialiseerd is in koppeling met Basisregistraties.
      KIK/AMC: Ook de kans op een datalek in deze verbinding is zeer klein. De connectie tussen RIVM en NICE wordt gelegd via een lijnencryptie. De data wordt versleuteld, zodat deze beveiligd overgedragen wordt. Er is een beperkt aantal mensen geautoriseerd. De geautoriseerde mensen moeten inloggen met een gebruikersnaam en een wachtwoord.
   D. T&T: Een lijst met combinatie van BSN, een Pid van de Stichting NICE, gemeentecode en geslacht van patiënten die in een ziekenhuis zijn opgenomen raakt publiek beschikbaar. Middels Pid zou koppeling met NICE mogelijk zijn, maar daarvoor moet tegelijkertijd een lek in de NICE-registratie aanwezig zijn.
      KIK/AMC: Een lijst met gegevens zoals genoemd in Hoofdstuk 2. Persoonsgegevens, gecombineerd met gemeentecode en geslachtsaanduiding

raakt openbaar beschikbaar. Hierin is BSN niet beschikbaar. PID wel, maar heeft slechts intern betekenis bij KIK/AMC. Het databestand is niet te koppelen met enig ander bestand.

5. Er komen meer gegevens beschikbaar dan alleen gemeentecode en geslachtsaanduiding
   A. Een combinatie van meerdere kenmerken van een persoon is onthullender, zeker in relatie met bijzondere persoonsgegevens
   B. Er is een te ruime bevraging van RIVM aan T&T
   C. Kans is zeer klein, want de web service kan beperkt worden tot de afgesproken gegevens
   D. Meer gegevens van betrokkene dan afgesproken is, kunnen bij RIVM terechtkomen.

Gegevens op het coronadashboard

1. Als er weinig mensen in het ziekenhuis liggen uit een gemeente, dan bestaat de kans dat gegevens alsnog herleidbaar worden.
   A. Dit kan betekenen dat herleidbaar is wie die ene persoon uit de gemeente is.
   B. Dit komt door het kleine aantal personen
   C. Gedurende de golf is deze kans relatief klein. Naarmate de crisis op zijn einde loopt wordt dit risico groter maar zal het nog relatief klein zijn omdat er ook andere mensen in het ziekenhuis liggen met andere klachten.
   D. Impact voor de betrokkenen zal beperkt zijn.

# D. Beschrijving voorgenomen maatregelen

In onderdeel D wordt bezien welke maatregelen kunnen worden getroffen om de in onderdeel C erkende risico's te voorkomen of te verminderen. Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de 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.**

1. Geen wettelijke grondslag voor verwerking BSN door KIK/AMC

De verwerkingsverantwoordelijke is de Stichting NICE en de verwerker is een afdeling van het AMC. Daarnaast is RIVM ook verwerker. RIVM koppelt middels BSN gemeentecode en geslachtsaanduiding aan de registratie. Zowel KIK/AMC als RIVM zijn op zichzelf gerechtigd BSN te verwerken. Echter de verrijkte gegevens door RIVM vloeien niet terug naar KIK/AMC. Het ministerie van VWS heeft bij brieven van 25 maart 2020 (medewerking registratie ivm COVID-19 epidemie NICE en LNAZ) en 7 augustus 2020 (Covid registratie in ziekenhuizen) aan de ziekenhuizen verzocht om de BSN-gegevens te delen met stichting NICE (KIK/AMC voor deze) ten behoeve van de correcte registratie. Het blijft een restrisico dat er verder gewerkt wordt met een verwerking van BSN die geen wettelijke grondslag heeft.

2. Foutief BSN

De pull door het RIVM is volledig geautomatiseerd om fouten ten aanzien van het BSN zo veel mogelijk te vermijden.

3. Gegevens worden langer bewaard dan noodzakelijk/BSN wordt niet verwijderd.

RIVM zal een procedure inregelen om dagelijks gemeentecode en geslacht toe te voegen waarbij het zo spoedig mogelijk, bij voorkeur automatisch, verwijderen van het BSN prioriteit heeft.

4. Er is sprake van een datalek.

Er wordt met extra beveiligde koppelingen gewerkt naar T&T waarbij de link slechts heel kort open staat en zo spoedig mogelijk afgesloten wordt. De koppeling van KIK/AMC naar RIVM is beveiligd met lijnencryptie. Gegevens worden versleuteld verstuurd. Ook hier staat de login slechts kort open. Zodra gegevens zijn betrokken wordt de link afgesloten.

5. Er worden meer gegevens uit de BRP getoond dan dat er worden opgevraagd.

Er komen bij het BRP meer gegevens beschikbaar dan de gevraagde gegevens
Er wordt in een strikt format alleen die gegevens alleen ruimte geboden voor die gegevens die opgevraagd worden. Er bestaat door deze systematiek geen ruimte voor extra informatie.

Gegevens op het coronadashboard

1. Kleine aantallen ziekenhuisopnamen per gemeente

Het risico is dusdanig beperkt dat er geen aanvullende maatregelen genomen worden. .

**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
persoonsgegeven
Risico's
minimaliseren
Richtinggevend
Rechtsgrond
Met open vizier

**Bijlage Advies** 5.1.2e **PIA CoronaDashboard**

Directie/concernonderdeel: VWS/RIVM
Naam 5.1.2e 5.1.2e
Contactgegevens: 5.1.2e @minvws.nl
Datum advies: 2 november 2020

## 1. Bronbestanden

- Gegevensbeschermingseffectbeoordeling –PIA Coronadashboard Versie 3.0, d.d. 2 oktober 2020

## 2. 5.1.2e Advies

5.1.2e is binnen het ministerie verantwoordelijk voor onafhankelijk toezicht op toepassing en naleving van de Algemene verordening gegevensbescherming. En heeft tot taak organisatieonderdelen te adviseren op uit te voeren en de uitgevoerde Gegevensbescherming effectboordeling - GEB, hierna te noemen PIA.

## 3. Uitgangspunten 5.1.2e Advies

Bij de review van onderliggende PIA is uitgegaan van de privacy beginselen volgens de AVG en een zo laag mogelijke privacy risico voor de betrokkenen[1], d.w.z. de opzet, inrichting en het gebruik heeft een zo laag mogelijke impact op de persoonlijke levenssfeer van de betrokkenen. Denk hierbij bijvoorbeeld aan:

- Verlies van controle over hun persoonsgegevens of de onmogelijkheid hun rechten en vrijheden uit te oefenen;
- Discriminatie, stigmatisering en uitsluiting
- (Blootstelling aan) identiteitsdiefstal of –fraude
- Gezondheidsschade
- Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens;
- Ongeoorloofde ongedaan making van pseudonimisatie;
- Enig ander aanzienlijk economisch of maatschappelijk nadeel

Als wel de bestuurlijke, politieke risico's die onrechtmatige verwerkingen met zich meebrengen.
De omgang met persoonsgegevens dienen te voldoen aan artikel 8 van het Handvest van de grondrechten van de Europese Unie (Handvest), artikel 16 van Verdrag betreffende de werking van de Europese Unie (VWEU), artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) en artikel 10 van de Grondwet.

Artikel 8 van het Handvest bepaalt onder meer dat persoonsgegevens eerlijk en voor bepaalde doeleinden moeten worden verwerkt, en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin

[1] De betrokkene is diegene van wie het de gegevens betreft.

de wet voorziet. Artikel 16 VWEU bepaalt dat eenieder in de Europese Unie recht heeft op bescherming van zijn persoonsgegevens. Op grond van artikel 8 EVRM is geen inmenging van enig openbaar gezag toegestaan in de uitoefening van het recht op respect voor zijn privéleven, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen. Artikel 10, eerste lid, van de Grondwet bepaalt dat eenieder recht heeft op eerbiediging van zijn persoonlijke levenssfeer, behoudens bij of krachtens de wet te stellen beperkingen.

Bij de toepassing van de in voornoemde grondrechtbepalingen opgenomen beperkingsclausules spelen het proportionaliteits- en het subsidiariteitsbeginsel een belangrijke rol. Deze beginselen volgen uit het woord 'noodzakelijk' zoals opgenomen in elk van de bovengenoemde grondslagen. Het proportionaliteitsbeginsel houdt in dat de inbreuken op de belangen van de bij de verwerking van persoonsgegevens betrokkene niet onevenredig mogen zijn in verhouding tot het met de verwerking te dienen doel. Ingevolge het subsidiariteitsbeginsel dient het doel waarvoor de persoonsgegevens worden verwerkt niet op een andere, voor de bij de verwerking van persoonsgegevens betrokkene minder nadelige, wijze te kunnen worden verwerkelijkt.

De belangrijkste uitgangspunten bij de review zijn:

- In hoeverre zijn de verantwoordelijkheden van de verschillende stakeholders inzichtelijk (verwerkingsverantwoordelijke, verwerker, sub verwerker).
- In hoeverre is de nut & noodzaak voldoende aantoonbaar aanwezig (art. 5, lid 1 c AVG);
- In hoeverre zijn de risico's van de gegevensverwerking (zowel voor gegevensuitwisseling, –opslag en gebruik) voor de rechten en vrijheden van de betrokkenen inzichtelijk, aantoonbaar en onderbouwd;
- In hoeverre is de gehele keten voldoende op privacy risico's verkend;
- In hoeverre is de gegevensverwerking rechtmatigheid; waaronder de grondslagen waarop de gegevensverwerking worden gebaseerd (art. 6 en art. 9 AVG);
- In hoeverre is zijn de proportionaliteit- en subsidiariteitsbeginselen toegepast en aantoonbaar;
- Minimale gegevensverwerking (dataminimalisatie) ten behoeve van zo'n laag mogelijke privacy risico's (art. 5, lid c AVG);
- Juistheid van de gegevens; dusdanige opzet en inrichting dat de juistheid van de gegevens gewaarborgd is (art. 5, lid 1 d AVG);
- In hoeverre is opslagbeperking t.a.v. bewaartermijnen dan wel dataminimalisatie aantoonbaar toegepast (art. 5, lid 1 e AVG);
- In hoeverre is het need-to-know principe gehanteerd (art. 5, lid 1 f AVG);

- Een veilige en betrouwbare gegevensuitwisseling, -opslag verwerking in lijn met wetgeving en relevante standaarden zoals de Code voor Informatiebeveiliging/ BIR-2017/BIO (art. 5, lid 1 f, en art. 24 AVG en art. 32 AVG) en voor wat betreft zorgsector (verwerking van gegevens over gezondheid) NEN 7510:2017 en in aanvulling daarop NEN7512:2015 en NEN 7513:2018.

## 4. Bevindingen

### Algemeen

Het verwerken van persoonsgegevens met als doel gegevens brengt inherente risico's voor gegevensbescherming met zich mee. De verantwoordelijkheid, de doeleinden en de grondslagen voor het ontvangen, opslaan en beschikbaar maken dient de DPIA duidelijk te beschrijven. Vervolgens dient de DPIA de verwerkingsverantwoordelijk te wijzen op de risico's en de maatregelen die de verwerkingsverantwoordelijke dient te nemen om de risico's te adresseren. Zodat de verwerkingsverantwoordelijke deze kan afwegen, waar mogelijk adresseren en eventueel accepteren.

Op basis van het vooradvies van 5.1.2e d.d. 9 oktober 2020 is de DPIA op een aantal punten aangescherpt en verduidelijkt. Dit betrof met name duidelijkheid verschaffen in de datastromen, de beveiliging, het autorisatiebesluit ten aanzien van het mogen koppelen van BSN aan BRP als RIVM zijnde als wel helderheid in de rechten van betrokkenen en de bewaartermijnen van de gegevens. De DPIA is op het vooradvies aangepast. 5.1.2e adviseert op basis van de aangepaste DPIA het volgende.

- **Gegevensbestanden (H.2);** Het verzamelen, verwerken, en delen van informatie tussen verschillende instanties is alleen toegestaan met inachtneming van de beginselen van noodzakelijkheid (artikel 8, tweede lid, van de EVRM) en dataminimalisatie (artikel 5, eerste lid, onder c, van de AVG). Deze beginselen eisen dat de hoeveelheid persoonsgegevens én het aantal betrokken personen tot het noodzakelijke worden beperkt. Het blijft onduidelijk welke gegevens zich in de afzonderlijke bestanden bevinden. Hierdoor is het niet scherp in hoeverre dataminimalisatie conform art. 5, lid c AVG wordt toegepast. Uit telefonisch contact met de projectleider blijken de bestand nr. 1 en 2 een redundantie aan gegevens van bestand 3 te bevatten. **Advies:** beperk de dubbelingen in de gegevensuitwisselingen om hiermee mogelijke privacy risico's te verkleinen.

- **Techniek en methode van gegevensverwerking (H.8);** Aangegeven staat dat de geautoriseerde datamanager voor de beveiligde omgeving moet inloggen met een gebruikersnaam en wachtwoord. Conform artikel 5 eerste lid onderdeel f AVG is de verwerkingsverantwoordelijke en de verwerker verplicht tot het treffen van passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen. Gezien de type gegevens is een beveiligingsniveau op basis van enkel gebruikersnaam en wachtwoord onvoldoende, wellicht zijn er nog andere beveiligingsmaatregelen getroffen tegen ongeoorloofde of onrechtmatige verwerking echter deze komen in de DPIA niet naar voren. Naast gebruik van een gebruikersnaam en wachtwoorden dient op zijn minst voorzien te zijn meerfactorauthenticatie. Naast de vereisten uit de AVG voldoet een dergelijk beveiligingsniveau niet aan de BIO – Baseline Informatiebeveiliging Overheid welke voor overheidsorganisatie vereist is. Meerfactorauthenticatie is een vorm van (toegangs)beveiliging waarbij de gebruiker zich met een combinatie van minimaal twee verschillende typen authenticatiefactoren moet authentiseren om toegang te krijgen tot de data.
  **Advies:** Pas meerfactorauthenticatie toe en maak duidelijk welke beveiligingsmaatregelen voor de beveiligde omgeving zijn toegepast.

- **Techniek en methode van gegevensverwerking (H.8).** In de DPIA staat aangegeven dat de data wordt versleuteld, zodat deze beveiligd kan worden overgedragen. Het is onduidelijk hoe met de sleutels voor het ontsleutelen wordt omgegaan en of hier mogelijke privacy risico's van toepassing zijn.
  **Advies:** Maak duidelijk hoe de gegevens versleuteld worden en hoe met de sleutels omgegaan wordt. Let op, het versleutelen van de data geldt niet alleen voor de gegevensuitwisseling maar wordt ook geadviseerd bij de opslag van de gegevens bij het RIVM.

- **Techniek en methode van gegevensverwerking (H.8).** In principe zijn stichting NICE via het mandaat van de ziekenhuizen om als verwerkingsverantwoordelijke op te treden en KIK/AMC als verwerkers verantwoordelijk voor de besloten, beveiligde omgeving van stichting NICE. Echter VWS/RIVM heeft hier een afhankelijkheid in dat deze beveiligde omgeving op een juiste wijze is beveiligd aangezien de gegevens t.b.v. VWS in de beveiligde omgeving geplaatst worden. Het is dan ook zaak om als VWS/RIVM zekerheid te hebben op het beveiligingsniveau van de beveiligde omgeving. De DPIA maakt niet inzichtelijk hoe het beveiligingsniveau van de beveiligde omgeving gewaarborgd is, bijvoorbeeld door een door NICE (te laten) uitgevoerde pentest, dan wel een beveiligingstest door de IT/securityafdeling van het RIVM zelf.
  **Advies:** Maak de beveiligingswaarborgen van de beveiligde omgeving inzichtelijk.

## 5. Reactie organisatieonderdeel op de bevindingen 5.1.2e

Bovenstaande adviezen zijn besproken met het RIVM als verwerkingsverantwoordelijke. RIVM heeft de adviezen geagendeerd en neemt hier zo spoedig mogelijk actie op. Voorwaarde hierbij is dat lopende vitale

processen doorgang kunnen blijven vinden. Het gaat hier onder meer om de dagelijkse aanlevering van data door de ziekenhuizen aan KIK/AMC alsmede doorlevering van de beschreven datasets door KIK/AMC aan het RIVM.