



Gegevensbeschermingseffectbeoordeling (PIA)

Ministerie van VWS

Publieke gezondheid/Programmadirectie COVID 19

Den Haag 2 oktober 2020



Ministerie van VWS - Publieke gezondheid/Programmadirectie COVID 19

Vaststelling verwerkersverantwoordelijke: 10 oktober 2020

Naam: 5.1.2e

Advies functionaris voor gegevensbescherming: 2 november 2020

Naam: 5.1.2e

Advies CIO: 2 november 2020

Naam: 5.1.2e

Ministerie van VWS - Publieke gezondheid/Programmadirectie COVID 19

Gegevensbeschermingseffectbeoordeling (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](mailto:5.1.2e@minvws.nl)

5.1.2e

Versie: 3.0, 27 oktober 2020

Inhoudsopgave

Inleiding.....	5
A. Beschrijving kenmerken gegevensverwerkingen.....	6
1. Voorstel	6
2. Persoonsgegevens	6
3. Gegevensverwerkingen	7
4. Verwerkingsdoeleinden	8
5. Betrokken partijen	9
6. Belangen bij de gegevensverwerking	10
7. Verwerkingslocaties	10
8. Techniek en methode van gegevensverwerking	11
9. Juridisch en beleidsmatig kader	11
10. Bewaartermijnen	12
B. Beoordeling rechtmatigheid gegevensverwerkingen.....	13
11. Rechtsgrond	13
12. Bijzondere persoonsgegevens	14
13. Doelbinding	14
14. Noodzaak en evenredigheid	15
15. Rechten van de betrokkene	17
C. Beschrijving en beoordeling risico's voor de betrokkenen.....	18
16. Risico's	18
D. Beschrijving voorgenomen maatregelen.....	20
17. Maatregelen	20

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 gegevensbeschermingseffectbeoordeling 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.

Klik hier om infotekst te verbergen

Beschrijf allereerst alle te verwerken categorieën van persoonsgegevens. Onder persoonsgegeven wordt verstaan: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.

Natuurlijke personen wil zeggen mensen. Informatie over overleden personen, rechtspersonen, dieren, zaken en objecten zijn in beginsel geen persoonsgegevens. Deze informatie kwalificeert weer wel als persoonsgegeven indien die ook betrekking heeft op een levende persoon.

Om te bepalen of iemand identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij kunnen worden gebruikt om de persoon te identificeren.

Gepseudonimiseerde (ook wel: versleutelde) gegevens worden als persoonsgegevens beschouwd. Onder pseudonimisering wordt verstaan: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens (sleutels) worden gebruikt. Hieraan wordt wel de eis verbonden dat deze aanvullende gegevens apart worden bewaard en maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een persoon worden gekoppeld.

Anonieme en geanonimiseerde gegevens zijn geen persoonsgegevens. Met anoniem en geanonimiseerd wordt bedoeld dat de persoon op wie het gegeven betrekking heeft, niet (meer) identificeerbaar is. Het anonimiseren van persoonsgegevens als zodanig is overigens weer *wel* een verwerking van persoonsgegevens.

Voorbeelden van persoonsgegevens zijn: naam, voorvoegsel, adres, telefoonnummer, e-mailadres, leeftijd, geboortedatum en -plaats, geslacht, woonplaats, nationaliteit, IP-adres, MAC-adres, KvK- nummer, voertuigidentificatienummer, winst eenmanszaak, bankrekeningnummer en -saldo, IQ, functie, opleiding, inkomens- en vermogensgegevens, kredietwaardigheid, persoonlijke voorkeuren, loonschaal, verslag van een functioneringsgesprek en (wan)gedrag. Ook metadata – informatie over informatie – zijn persoonsgegevens als hieruit de identiteit van de betrokkene kan worden herleid. Voorbeelden van metadata zijn: welke browser of telefoon iemand gebruikt, wanneer een document is opgesteld of voor het laatste bewerkt en de geschreven taal. Ook locatie-informatie en geografische informatie kwalificeren als persoonsgegevens als de informatie herleidbaar is tot een persoon. Denk hierbij aan de koppeling van gegevens uit de basisregistratie adressen en gebouwen aan andere gegevens en het monitoren van de locaties van voertuigen.

Typen

Stel vervolgens de aard van de te verwerken categorieën van persoonsgegeven vast. De AVG onderscheidt drie typen van persoonsgegevens – gewone, bijzondere en strafrechtelijke persoonsgegevens – en stelt verschillende eisen aan een rechtmatige verwerking daarvan. De gedachte hierachter is dat hoe gevoeliger de aard van de persoonsgegevens, hoe groter de effecten voor de betrokkenen zijn.

Bijzondere persoonsgegevens

Hieronder een limitatieve opsomming van categorieën van bijzondere persoonsgegevens:

- ras of etnische afkomst;
- politieke opvattingen;
- religieuze of levensbeschouwelijke overtuigingen;
- het lidmaatschap van een vakbond;
- genetische gegevens;
- biometrische gegevens met het oog op de unieke identificatie van een persoon;
- gegevens over gezondheid;
- gegevens over seksueel gedrag of seksuele gerichtheid.

Voorbeelden van bijzondere persoonsgegevens zijn: het adressenbestand van een kerkblad, gegevens die via een apothekers-app worden verwerkt, ziekte- en verzuimgegevens van werknemers, ledenlijst van een politieke partij, relaties op sociale media. Let op: uit beeldmateriaal zoals foto's en camerabeelden kunnen soms ook bijzondere persoonsgegevens, zoals etnische afkomst of medische gesteldheid, worden afgeleid.

Genetische gegevens

Genetische gegevens zijn persoonsgegevens over overgeërfde of verworven genetische kenmerken van een persoon die unieke informatie verschaffen over zijn fysiologie of gezondheid en die met name voortkomen uit een analyse van een biologisch monster van die persoon. Denk hierbij aan: chromosomen, DNA of RNA en erfelijke ziekten.

Biometrische gegevens

Biometrische gegevens zijn persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met fysieke, fysiologische of gedragsgerelateerde kenmerken van een persoon op grond waarvan eenduidige identificatie van die persoon mogelijk is of wordt bevestigd. Denk hierbij aan: vingerafdrukken, irispatroon, gezichtsprofiel, toetsaanslaganalyse, looppatroon, stemgeluid en slaapritme. Foto's vallen overigens alleen onder de definitie van biometrische gegevens wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie mogelijk maken.

Gegevens over gezondheid

Gezondheidsgegevens zijn persoonsgegevens over de fysieke of mentale gezondheid van een persoon. Denk hierbij aan: gewicht, hartaanval, handicap, ziekterisico of verleende gezondheidsdiensten.

Strafrechtelijke persoonsgegevens

Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen (hierna: strafrechtelijke persoonsgegevens) zijn een apart type persoonsgegeven. Het gaat hier zowel om veroordelingen als om verdenkingen van strafbare feiten. Voorbeelden hiervan zijn: proces-verbaal, sepotbeslissing, strafblad, relaas verhoor en aanvraag voor een toevoeging in een strafzaak.

Wettelijke identificatienummers

Nummers ter identificatie van een persoon die bij wet zijn voorgeschreven, mogen slechts worden verwerkt voor doeleinden die bij wet zijn bepaald. De gedachte hierachter is dat persoonsnummers de koppeling van verschillende bestanden aanzienlijk vergemakkelijken en daarmee een extra bedreiging voor de persoonlijke levenssfeer vormen. Denk hierbij aan: een burgerservicenummer (BSN), BIGnummer (beroepen in de individuele gezondheidszorg), A-nummer (basisregistratie personen), onderwijsnummer, strafrechtkenummer en kenteken. Het gaat hierbij enkel om in de wet voorgeschreven persoonsidentificerende nummers.

Overige persoonsgegevens

Alle overige persoonsgegevens die niet kwalificeren als bijzonder of strafrechtelijk worden in dit model aangemerkt als gewone persoonsgegevens. Gewone persoonsgegevens wil overigens niet zeggen dat geen sprake is van een hoog privacyrisico. Bepaalde persoonsgegevens kunnen door de context waarin zij worden gebruikt gevoelig zijn en daardoor een hoog privacyrisico met zich brengen. Hierbij kan gedacht worden aan:

- gegevens over de financiële of economische situatie van de betrokkene;
- gegevens over overtredingen van wettelijke voorschriften, bestuurlijke en/of tuchtrechtelijke maatregelen of sancties;
- (andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
- gegevens die betrekking hebben op kwetsbare groepen;
- gebruikersnamen, wachtwoorden en andere inloggegevens;

- gegevens die kunnen worden misbruikt voor (identiteits)fraude;
- communicatie en locatiegegevens.

Betrokkenen

Benoem tot slot de categorieën van betrokkenen van wie de persoonsgegevens worden verwerkt. Denk hierbij aan: medewerkers, consumenten, cliënten, patiënten, zakelijke contacten, bezoekers, gebruikers of ingezetenen van een gemeente. De omvang en categorie van betrokkenen kunnen invloed hebben op de effecten van het voorstel. Bepaalde betrokkenen zijn kwetsbaarder dan anderen. Met kwetsbaar wordt bedoeld dat de negatieve effecten van een (onrechtmatige) gegevensverwerking groter kunnen zijn voor bepaalde betrokkenen dan voor andere (zie ook de anderszins gevoelige persoonsgegevens). Denk bijvoorbeeld aan: minderjarigen, verstandelijk gehandicapten, mensen die te maken hebben met stalking of die in een blijf-van-mijn-lijfhuis verblijven, medewerkers van inlichtingen- en veiligheidsdiensten, klokkenluiders of informanten van politie of justitie. Betrokkenen hebben op grond van de privacyregulering bepaalde rechten, zoals het inzage- en correctierecht.

De AVG biedt specifieke bescherming aan kinderen, omdat zij zich minder bewust zullen zijn van de effecten van de gegevensverwerking en van hun rechten in dat kader. Die specifieke bescherming geldt met name voor het gebruik van persoonsgegevens van kinderen voor marketingsdoeleinden, het opstellen van persoonlijkheids- of gebruikersprofielen en het verzamelen van persoonsgegevens over kinderen bij het gebruik van rechtstreeks aan kinderen verstrekte diensten. Zo is wanneer het kind jonger is dan 16 jaar zo'n verwerking slechts rechtmatig, indien de toestemming of machtiging tot toestemming wordt verleend door de ouder of voogd. Ook heeft de leeftijd van betrokkenen gevolgen voor de wijze waarop hij geïnformeerd moet worden.

In het kader van de Richtlijn kan het onderscheid worden gemaakt tussen:

- personen ten aanzien van wie gegronde vermoedens bestaan dat zij een strafbaar feit hebben gepleegd of zullen plegen;
- personen die voor een strafbaar feit zijn veroordeeld;
- slachtoffers van een strafbaar feit, of personen ten aanzien van wie bepaalde feiten aanleiding geven tot het vermoeden dat zij het slachtoffer zouden kunnen worden van een strafbaar feit; en
- andere personen die bij een strafbaar feit betrokken zijn, zoals personen die als getuige kunnen worden opgeroepen in een onderzoek naar strafbare feiten of een daaruit voortvloeiende strafrechtelijke procedure, personen die informatie kunnen verstrekken over strafbare feiten, of personen die contact hebben of banden onderhouden met een van de personen bedoeld onder a en b.

Bij **conceptregulering** kan het wenselijk zijn om de te verwerken categorieën van persoonsgegevens in de regeling op te nemen. Wanneer de verwerking onder de werkingssfeer van de Richtlijn valt, is het verplicht om de te verwerken categorieën van persoonsgegevens in de regeling op te nemen.

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 Informatics) 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.

Klik hier om infotekst te verbergen

De privacyregelgeving geeft als beginsel dat persoonsgegevens enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld. De vaststelling van de verwerkingsdoeleinden is een noodzakelijk voorwaarde om te kunnen beoordelen of de voorgenomen gegevensverwerkingen rechtmatig zijn (onder B) en om vast te stellen welke maatregelen moeten worden getroffen om de risico's (onder C) te voorkomen of verkleinen (onder D). Omschrijf daarom per voorgenomen gegevensverwerking de verwerkingsdoeleinden zo specifiek mogelijk.

Bij verwerkingsdoeleinden kan gedacht worden aan: beveiligen van gebouwen en objecten, behandelen van personeelszaken, opsporen van strafbare feiten, direct marketing, het innen van vorderingen, het doen van leveringen en bestellingen, identificatie en authenticatie, het voorbereiden en nemen van Awb-besluiten en het behandelen van geschillen. Denk ook aan eventuele nevendoeleinden van de gegevensverwerking, zoals: wetenschappelijk, statistisch of historisch onderzoek, archiefbeheer, declaratiedoeleinden, rapportagedoeleinden, verbetering van dienstverlening of (door)ontwikkeling van beleid. De verwerkingsdoeleinden moeten zoveel mogelijk worden toegesplitst op de concrete gegevensverwerking, waarbij het algemene overkoepelende doel kan worden gebruikt als kapstok waaraan verschillende subdoelen kunnen worden gehangen, bijvoorbeeld:

- e-mailadres: noodzakelijk voor communicatie met betrokkene;
- ip-adres: noodzakelijk ter verificatie dat alleen vanuit een bepaalde locatie contact wordt gemaakt met het systeem;
- adresgegevens: noodzakelijk om een beschikking naar de betrokkene te kunnen toezenden;
- financiële gegevens: noodzakelijk om vast te stellen of de betrokken partij in aanmerking komt voor een toeslag;
- strafrechtelijke gegevens: noodzakelijk om een screening te kunnen uitvoeren.

Wanneer de persoonsgegevens niet rechtstreeks bij de betrokkene worden verkregen (met andere woorden: de

persoonsgegevens zijn afkomstig van een andere persoon of organisatie dan wel uit een bestaand databestand), is het noodzakelijk om de doeleinden waarvoor de gegevens oorspronkelijk zijn verzameld te herleiden. De privacyregelgeving geeft namelijk als beginsel dat persoonsgegevens niet verder mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Met andere woorden: de verwerking van persoonsgegevens voor andere doeleinden dan die waarvoor de persoonsgegevens aanvankelijk zijn verzameld, mag enkel indien de verwerking verenigbaar is met de doeleinden waarvoor de persoonsgegevens aanvankelijk zijn verzameld (zie voor de beoordeling van de verenigbaarheid punt 13 hieronder). Met verdere verwerking wordt bedoeld op gebruik van persoonsgegevens die al eerder voor een bepaald doel zijn verzameld. Denk hierbij aan verstrekkingen van persoonsgegevens aan een andere organisatie die niet oorspronkelijk, ten tijde van het verzamelen van de gegevens, was beoogd.

Bij **conceptregelgeving** wordt het doel van de gegevensverwerking in de regeling zelf vastgelegd of op zijn minst benoemd in de memorie of nota van toelichting. Een wettelijke doelomschrijving bevordert de rechtszekerheid omdat hierdoor een nadere invulling is gegeven aan het beoordelingskader.

Bij **overheidsverwerkingen** stelt de verwerkingsverantwoordelijke het doel van de gegevensverwerkingen zelf vast. Bij overheidsverwerkingen ter uitvoering van regelgeving moet binnen het doel worden gebleven dat daarin is vastgesteld. Het verdient de voorkeur de verwerkingsdoeleinden zoveel mogelijk op het niveau van werk- en organisatieprocessen te enten.

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. Ziekenhuisopnames 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 geboortjaar 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 geboortjaar 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 Informatics) 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 betreft 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, geboortjaar 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 betreft. 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.

[Klik hier om infotekst te verbergen](#)

Gebruikmaking van bepaalde technieken en methoden van gegevensverwerking kunnen aanvullende privacyrisico's met zich brengen en daarom onderworpen zijn aan strengere regels en aanvullende maatregelen vereisen. Dit is onder meer het geval bij (semi-)geautomatiseerde besluitvorming, profilering en big data-verwerkingen.

Geautomatiseerde besluitvorming

Uitsluitend op geautomatiseerde verwerking gebaseerde besluiten die voor de betrokkenen rechtsgevolgen hebben of hem anderszins in aanmerkelijke mate treffen, zijn in beginsel verboden.

Voor verwerkingen die onder de werkingssfeer van de AVG vallen, geldt dat dit verbod niet van toepassing indien het besluit:

- noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;
- is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene; of
- berust op de uitdrukkelijke toestemming van de betrokkene.

Bij verwerkingen die vallen onder de werkingssfeer van de Richtlijn geldt dit verbod niet indien het besluit:

- wettelijk is toegestaan; en
- voorziet in passende waarborgen voor de rechten en vrijheden van de betrokkenen, waaronder ten minste het recht op menselijke tussenkomst.

Profilering

Onder profilering wordt verstaan: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

Bepaalde gegevens, zoals de resultaten van een zoekopdracht met een zoekmachine, kunnen in combinatie met elkaar een risicoprofiel doen ontstaan. De kans hierop bestaat vooral wanneer meerdere registers met elkaar worden gecombineerd. Er kan sprake zijn van profilering wanneer:

- op basis van een combinatie van persoonsgegevens, zoals het automerk in combinatie met de leeftijd van de betrokkene wordt besloten iemand extra te controleren;
- gebruik wordt gemaakt van de gegevens die websitebezoekers achterlaten om de doelgroep van de website mee vast te stellen.

Bij verwerkingen die vallen onder de werkingssfeer van de Richtlijn, geldt dat profilering die leidt tot discriminatie op grond bijzondere persoonsgegevens verboden is.

Big data

Big data is als zodanig niet gedefinieerd in de privacyregelgeving, maar hangt als verschijnsel nauw samen met geautomatiseerde besluitvorming en profilering. *Big data* staat voor het verschijnsel dat grote hoeveelheden gestructureerde en ongestructureerde data uit verschillende bronnen worden geanalyseerd waarbij geautomatiseerd naar correlaties wordt gezocht die kennis kunnen opleveren om te kunnen toepassen voor beslissingen op groeps- of individueel niveau. In de kern komt het bij *big data*-analyses neer op het zoeken naar correlatie (onderlinge samenhang tussen twee reeksen van waarnemingen), in tegenstelling tot causaliteit (betrekking van oorzaak en gevolg). Toepassing van *big data* brengt specifieke risico's mee en vergt daarom ook specifieke maatregelen (zie onder D).

Nieuwe technologieën

Ook grote verschuivingen in de werkwijze, de manier waarop persoonsgegevens worden verwerkt en de technologie die daarbij gebruikt wordt, kunnen gevolgen hebben voor betrokkenen. Denk aan: intelligente volgsystemen op basis van GPS, biometrie en nieuwe vormen van identificatie.

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.

[Klik hier om infotekst te verbergen](#)

De privacyregelgeving geeft als beginsel dat persoonsgegevens niet langer in een vorm die het mogelijk maakt de betrokkenen te identificeren, mogen worden bewaard dan voor de verwezenlijking van de verwerkingsdoeleinden noodzakelijk is. Met andere woorden: indien het voor de verwezenlijking van de verwerkingsdoeleinden niet meer noodzakelijk is de persoonsgegevens te bewaren, moeten deze worden vernietigd of geanonimiseerd. Op dit beginsel van opslagbeperking maakt de privacyregelgeving een uitzondering indien de persoonsgegevens uitsluitend worden verwerkt ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. Hieraan wordt wel de eis verbonden dat passende maatregelen worden getroffen om de betrokkenen te beschermen.

Bij **conceptregelgeving** zal moeten worden bepaald en gemotiveerd of het al dan niet wenselijk is om een specifieke minimale of maximale bewaartermijn voor te schrijven. Aan de hand van het uitgangspunt dat de bewaartermijn in verhouding moet staan met de verwerkingsdoeleinden, moet de gekozen termijn worden

gemotiveerd. Motiveer ook het niet opnemen van een bewaartermijn.

Bij **overheidsverwerkingen** moet worden nagegaan of regelgeving een bewaartermijn voorschrijft. Indien dat het geval is, moet de verwerkingsverantwoordelijke zich aan die termijn houden. Indien geen wettelijke bewaartermijn is voorgeschreven, moet de verwerkingsverantwoordelijke zelf bewaartermijnen vaststellen of de gegevens periodieke toetsen aan het beginsel van opslagbeperking.

Hierbij moet rekening worden gehouden met andere regelgeving over bewaartermijnen, zoals de Archiefwet 1995.

Voorbeeld opsomming bewaartermijn voor persoonsgegevens bij overheidsverwerkingen (IT/uitvoering):

Categorie Persoonsgegeven	Ingang bewaartermijn	Termijn van bewaring	Motivatie bewaring	Verantwoordelijkheid voor verwijdering
Naam	Vanaf moment dat de betrokkene voor het eerst inlogt in het systeem.	365 dagen, als de gebruiker 'onthouden inloggegevens' aanklikt 30 dagen.	Deze persoonsgegevens zijn functioneel: het gegeven zorgt er voor dat je met slechts één handeling inlogt in het verschillende databases.	Functioneel beheerder

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.

1.1. Rechtsgrond



Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.

[Klik hier om infotekst te verbergen](#)

De AVG geeft als beginsel dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. Als uitwerking van dit beginsel is geregeld dat een gegevensverwerking alleen rechtmatig is indien deze gebaseerd kan worden op ten minste één van de volgende zes rechtsgronden:

- a. de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
- b. de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
- c. de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
- d. de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
- e. de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
- f. de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

Of de gegevensverwerkingen noodzakelijk zijn, wordt beoordeeld onder punt 14.

Ten aanzien van de rechtsgronden c (wettelijke plicht) en e (taak van algemeen belang) geldt dat deze moet

worden vastgesteld bij of krachtens de wet. De wettelijke verplichting (rechtsgrond c) hoeft niet noodzakelijkerwijs te bestaan uit een expliciete verplichting om persoonsgegevens te verwerken. Ook is mogelijk dat de verwerking van persoonsgegevens een basis vindt in een ruimer geformuleerde zorgplicht of wettelijke verplichting. Zonder verwerking van de persoonsgegevens moet het uitvoeren van een wettelijke verplichting redelijkerwijs niet goed mogelijk zijn. Met betrekking tot rechtsgrond e (de taak van algemeen belang) geldt dat deze taak zal moeten blijken uit regelgeving die op de verwerkingsverantwoordelijke van toepassing is. Niet noodzakelijk is dat in de regelgeving ook expliciet is opgenomen dat ten behoeve van de vervulling van de wettelijke taak gegevens verwerkt mogen worden. Indien het noodzakelijk is om voor de uitvoering van de publieke taak persoonsgegevens te verwerken, kan de wettelijke grondslag voor de publieke taak tevens worden beschouwd als grondslag voor de verwerking van persoonsgegevens.

De Richtlijn gegevensbescherming opsporing en vervolging voor dat een gegevensverwerking door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid alleen rechtmatig is indien die verwerking gebaseerd is op de wet.

Bij **conceptregelgeving** zal de regeling veelal tot gevolg hebben dat de verwerkingsverantwoordelijke de gegevensverwerking kan baseren op de rechtsgrond genoemd onder c (wettelijke verplichting). Dit is het geval indien de gegevensverwerking noodzakelijk is ter uitvoering van de wettelijke verplichting en indien de verwerkingsverantwoordelijke belast is met de uitvoering van de wettelijke plicht. Daarnaast kan regelgeving tot gevolg hebben dat een overheidsorgaan de gegevensverwerking kan baseren op de rechtsgrond genoemd onder e (taak van algemeen belang). De publieke taak wordt (of is reeds) wettelijk vastgelegd waarbij, naast andere onderwerpen, volgens de Aanwijzingen voor de regelgeving ook aandacht moet worden geschonken aan de daarbij noodzakelijke gegevensverwerkingen. In regelgeving kan ook worden voorgeschreven dat toestemming van de betrokkene vereist is om persoonsgegevens te verwerken, en daarmee de andere rechtsgronden uitsluiten.

Bij **overheidsverwerkingen** zal het overheidsorgaan de voorgenomen gegevensverwerkingen moeten baseren op één van de zes rechtsgronden. De rechtsgrond genoemd onder f geldt niet voor gegevensverwerkingen in het kader van de uitoefening van publieke taken. Wel kan deze rechtsgrond gebruikt worden voor gegevensverwerkingen in de bedrijfsvoering, zoals cameratoezicht, bezoekersregistratie en toegangscontrole. In veel situaties zal de rechtsgrond genoemd onder a (toestemming) evenmin kunnen dienen als rechtsgrond voor gegevensverwerkingen door overheidsorganen, omdat de betrokkene in de gegeven situatie niet vrijelijk toestemming kan geven.

Indien de gegevensverwerkingen gebaseerd worden op de rechtsgrond genoemd onder f (het gerechtvaardigd belang van de verwerkingsverantwoordelijke of een derde), dan stelt de AVG als eis dat de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene niet zwaarder mogen wegen dan de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of de derde.

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.

[Klik hier om infotekst te verbergen](#)

De privacyregelgeving geeft als beginsel dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden moeten worden verzameld en vervolgens niet verder mogen worden verwerkt op een met die doeleinden onverenigbare wijze.

De AVG regelt dat de verdere verwerking voor een ander doel toegestaan is indien de verdere verwerking berust op toestemming van de betrokkene of op een specifiek wettelijk voorschrift, dat een noodzakelijke en evenredige maatregel is in een democratische samenleving ter waarborging van een belangrijke doelstelling van algemeen belang, bijvoorbeeld de nationale veiligheid, de openbare veiligheid, monetaire, budgettaire of fiscale

aangelegenheden. Daarnaast wordt de verdere verwerking ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden als verenigbaar geacht met de oorspronkelijke doeleinden. Hieraan wordt wel de eis verbonden dat passende maatregelen worden getroffen om de betrokkene te beschermen.

Bij **conceptregelgeving** moet worden beoordeeld of het noodzakelijk is om wettelijk te regelen dat verdere verwerking toegestaan is (zie ook punt 14 hierna), bijvoorbeeld in verband met de doorbreking van een geheimhoudingsplicht.

Binnen het hierboven geschetste kader voor verwerking voor een ander doel bestaat ruimte voor een wettelijke regeling op grond waarvan sets van persoonsgegevens van meerdere partijen uit meerdere domeinen worden gecombineerd ten behoeve van een big data analyse, waarbij gegevens worden verwerkt ten behoeve van een in die wettelijke regeling vastgesteld doeleinde, dat niet met het oorspronkelijke doel waarvoor de gegevens zijn verzameld, verenigbaar is. Dit laat onverlet dat de verwerkingsverantwoordelijke die beslissingen neemt ten aanzien van individuele personen of een groep van personen op basis van de uitkomsten van die analyse zelfstandig moet voldoen aan alle eisen voor rechtmatige gegevensverwerking. Een dergelijke verwerking dient op een eigen rechtsgrond te berusten (zie punt 11).

Bij **overheidsverwerkingen** moet de verwerkingsverantwoordelijke zelf beoordelen of de verdere gegevensverwerking voor een ander doel toegestaan en verenigbaar is aan de hand van:

- a. het verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld en de doeleinden van de voorgenomen verdere verwerking;
- b. de context waarin de persoonsgegevens zijn verzameld, met name wat de verhouding tussen de betrokkene en de verwerkingsverantwoordelijke betreft;
- c. de aard van de persoonsgegevens, met name bijzondere of strafrechtelijke persoonsgegevens;
- d. de mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkene;
- e. het bestaan van passende waarborgen.

De Richtlijn staat de verdere verwerking van persoonsgegevens toe voor een doelstelling die binnen het toepassingsgebied van de Richtlijn valt, niet zijnde die waarvoor zij zijn verzameld, voor zover:

- a. de verwerkingsverantwoordelijke overeenkomstig de wet gemachtigd is deze persoonsgegevens voor een dergelijk doel te verwerken; en
- b. de verwerking noodzakelijk is en in verhouding staat tot dat andere doel.

De verdere verwerking voor andere doeleinden is enkel op basis van de wet toegestaan. Wanneer de persoonsgegevens voor zulke andere doeleinden worden verwerkt, is de AVG van toepassing.

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 voorgenen 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 uitezette 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.

[Klik hier om infotekst te verbergen](#)

Betrokkenen hebben op grond van de privacyregelgeving diverse rechten, waarin ook staat op welke wijze en onder welke omstandigheden zij die rechten kunnen uitoefenen. Het betreft het recht op informatie, het recht van inzage, het recht op rectificatie, het recht op gegevenswissing, het recht op beperking van de verwerking, een kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens, het recht op overdraagbaarheid van gegevens, het recht van bezwaar en het recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit. Er zijn uitzonderingen mogelijk op de uitoefening van deze rechten, op voorwaarde dat de wezenlijke inhoud van de grondrechten en fundamentele vrijheden niet wordt aangetast en dat het gaat om noodzakelijke en evenredige maatregelen ter waarborging van enkele expliciet opgesomde belangrijke doelstellingen van algemeen belang. Uitzonderingen moeten altijd op een nationale wet berusten, direct zijn toegestaan op grond van de bepalingen in de Europese privacyregelgeving.

Indien in conceptregelgeving een uitzondering wordt gemaakt op de rechten van betrokkenen moet worden beoordeeld of dit is toegestaan op in de privacyregelgeving genoemde gronden én moeten specifieke bepalingen worden opgenomen met betrekking tot ten minste:

- de verwerkingsdoeleinden;
- de categorieën van persoonsgegevens;
- het toepassingsgebied van de ingevoerde beperkingen;

- d. de waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte
- e. de specificatie van de verwerkingsverantwoordelijke of de categorieën van verwerkingsverantwoordelijken;
- f. de opslagperiodes en de toepasselijke waarborgen;
- g. de risico's voor de rechten en vrijheden van betrokkenen;
- h. het recht van betrokkenen om over de beperking te worden geïnformeerd, tenzij dit afbreuk kan doen aan het doel van de beperking.

Geef bij **overheidsverwerkingen** aan hoe invulling wordt gegeven aan de rechten van betrokkenen, bijvoorbeeld op welke wijze de betrokkenen worden geïnformeerd en hoe wordt omgegaan met een aanvraag voor correctie en wissing van gegevens. Indien de verwerkingsverantwoordelijke uitzonderingen wil maken op de uitoefening van bepaalde rechten van betrokkenen, geef aan waarom dat noodzakelijk is en op welke grond 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 geslachtsaanduiding 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: Modelleren

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.**

Klik hier om infotekst te verbergen

Volgens de privacyregelgeving dient een PIA een beoordeling van risico's voor de rechten en vrijheden van de betrokkenen te bevatten. Aan de hand van de aard, het toepassingsgebied, de context en de doeleinden van de gegevensverwerking dient de waarschijnlijkheid en de ernst van het risico voor de rechten en vrijheden van de betrokkenen te worden bepaald. Op basis van een objectieve beoordeling kan vastgesteld worden of de gegevensverwerking gepaard gaat met een (hoog) risico. Hiervoor is het nodig om de oorsprong, de aard, het specifieke karakter en de ernst van dat risico te evalueren.

Het gaat hier om een risicogerichte benadering die kan bestaan uit de volgende stappen:

1. risico's identificeren;
2. risico's inschatten/analyseren;
3. risico's beoordelen/evalueren.

Deze benadering zal in grote lijnen vergelijkbaar zijn met een risicoafweging in het kader van informatiebeveiliging. Daarom kan ook gebruik gemaakt worden van informatie die daaruit naar voren is gekomen. Anders dan bij deze risicoafweging die gericht is op de betrouwbaarheidseisen voor informatiesystemen, en daarmee de risico's voor de verantwoordelijke (zoals aanpassing, vertrouwen, publiciteit, toezicht en handhaving, dienstverlening, betrouwbare informatie), ziet de risicoafweging van de PIA op de risico's voor de betrokkenen.

De privacyregelgeving schrijft niet voor op welke wijze de risicoanalyse moet worden uitgevoerd. Het verdient aanbeveling om aan te sluiten bij internationale standaarden, bijvoorbeeld van de International Organization of Standardization (ISO), Eenduidige Normatiek Single Information Audit (ENSIA) en Organisation for Economic Co-operation and Development (OECD).

1. Risico's identificeren

De eerste stap is om potentiële privacyrisico's vast te stellen. Een privacyrisico is een kans op het optreden van

een negatief gevolg voor de rechten en vrijheden van de betrokkenen als gevolg van de verwerking van persoonsgegevens.

Bij rechten en vrijheden van de betrokkenen moet in eerste instantie aan het recht op privacy worden gedacht, maar ook aan andere fundamentele rechten en vrijheden, zoals de vrijheid van meningsuiting, de vrijheid van godsdienst en het verbod van discriminatie. Het voordoen van de (hypothetische) situatie kan leiden tot lichamelijke, materiële of immateriële schade voor de betrokkene. Hierbij kan gedacht worden aan de volgende situaties:

- * waar de gegevensverwerking kan leiden tot:
 - discriminatie, stigmatisering en uitsluiting;
 - (blootstelling aan) identiteitsdiefstal of -fraude;
 - financiële verliezen;
 - reputatie- of anderszins relationele schade;
 - verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens;
 - ongeoorloofde ongedaanmaking van pseudonimisering;
 - of enig ander aanzienlijk economisch of maatschappelijk nadeel voor de natuurlijke persoon in kwestie;
 - wanneer de betrokkenen hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd om controle over hun persoonsgegevens uit te oefenen;
 - wanneer bijzondere of strafrechtelijke persoonsgegevens worden verwerkt;
 - wanneer persoonlijke aspecten worden geëvalueerd, om bijvoorbeeld beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen te analyseren of te voorspellen, teneinde persoonlijke profielen op te stellen of te gebruiken;
 - wanneer persoonsgegevens van kwetsbare personen, zoals kinderen, worden verwerkt; of
 - wanneer de verwerking een grote hoeveelheid persoonsgegevens betreft en gevolgen heeft voor een groot aantal betrokkenen.

2. Risico's inschatten

Vervolgens moeten de benoemde risico's worden gekwalificeerd door het inschatten van de kans dat een dreiging zich voordoet en de mogelijke gevolgen daarvan voor de betrokkenen. Met andere woorden: wat zijn de gevreesde gevolgen en hoe groot is de impact daarvan op de betrokkenen? En hoe treden deze in werking en hoe waarschijnlijk is dat? Deze vragen zijn niet gericht op zwart-wit antwoorden, maar op een afweging. Aan de hand hiervan moet een risiconiveau worden bepaald.

De impact/ernst van de risico's hangt af van de context van de verwerkingen: de aard van de persoonsgegevens, de aard van de verwerkingen en de doeleinden waarvoor de gegevens worden verwerkt.

De kans dat de risico's zich voltrekken is mede afhankelijk van de middelen die de verwerkingsverantwoordelijke gebruikt bij de gegevensverwerking. Alsook van de aard van de persoonsgegevens.

Persoonsgegevens die de sleutel vormen voor toegang tot geldelijke middelen of waarmee een betrokkene te chanteren is, zijn aantrekkelijk voor hackers. Denk hierbij aan de inloggegevens voor DigiD of een datingwebsite.

De kans dat zich gevolgen voordoen voor de rechten en vrijheden van de betrokkenen, kan tevens verband houden met de (mate van) beveiliging van de persoonsgegevens. De al dan niet opzettelijke:

- vernietiging en verlies (beschikbaarheid);
 - wijziging (integriteit);
 - ongeoorloofde toegang en verstrekking (vertrouwelijkheid);
- van persoonsgegevens, kan leiden tot schade voor de betrokkene.

Voor het inschatten van de risico's kan het behulpzaam zijn om de betrokkenen of hun vertegenwoordigers te consulteren.

Big data-verwerkingen kunnen specifieke risico's voor de betrokkene met zich brengen. Zo kan een algoritme een correlatie ontdekken die weliswaar in statistische zin logisch is, maar die kan leiden tot vooroordelen en stereotypering, discriminatie en sociale uitsluiting of anderszins impact heeft op de betrokkenen, bijvoorbeeld bij sollicitaties, het aangaan van leningen en afsluiten van verzekeringen.

Ook bestaat het risico dat de betrokkene onderworpen is aan big data-besluitvorming die hij niet begrijpt en waar hij geen invloed op heeft.

3. Risico's beoordelen

Definieer aanvaardbare risicowaarden en beoordeel of de risico's aanvaardbaar zijn.

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.
 - E.
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 E.
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 betrouwbare 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 lijncryptie. 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 terecht komen.
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 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.

[Klik hier om infotekst te verbergen](#)

Denk bij maatregelen bijvoorbeeld aan: het extra informeren van de betrokkenen, een extra keuze-, inspraak- of bezwaarmogelijkheid voor de betrokkenen, periodieke controles, toezicht verstevigen, verhogen bewustwording en dataminimalisatie.

Daarnaast kunnen de maatregelen ook beveiligingsmaatregelen omvatten. De privacyregelgeving geeft als beginsel dat persoonsgegevens door het nemen van passende technische en organisatorische maatregelen op een dusdanige manier wordt verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

De verwerkingsverantwoordelijk moet passende technische en organisatorische maatregelen treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. In het begrip passend ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek. Het begrip passend duidt mede op een proportionaliteit tussen de maatregelen en erkende privacyrisico's. Naarmate de risico's groter zijn, worden zwaardere eisen gesteld aan de beveiliging van de persoonsgegevens. Er is geen verplichting om altijd de zwaarste beveiliging te nemen. Enkel is vereist dat de maatregelen met het oog op de beschikbare technologie en uitvoeringskosten redelijk zijn. Deze maatregelen moeten het risico tot een aanvaardbaar niveau brengen. Beveiligingsrisico's volledig reduceren is niet mogelijk. Dit betekent dat er altijd een restrisico zal overblijven. De verwerkingsverantwoordelijke dient te beschrijven hoe hij tot dit restrisico is gekomen en waarom dit aanvaardbaar wordt geacht.

Een passend beveiligingsniveau veronderstelt dat gewerkt wordt met een planning- en controlcyclus (plan-do-check-act) aan de hand waarvan kan worden beoordeeld of de beveiliging steeds adequaat is voor de huidige stand van de techniek en de organisatie.

Voor te treffen maatregelen kan worden aangehaakt bij beveiligingskaders en -standaarden, beste praktijken en goedgekeurde gedragscodes en certificeringsmechanismen.

Ter illustratie noemt de AVG de volgende maatregelen:

- pseudonimiseren en versleutelen van persoonsgegevens;
- het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de

- verwerkingssystemen en diensten te garanderen;
- c. het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
 - d. een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Daarnaast kan worden gedacht aan de volgende maatregelen, mede bedoeld om ervoor te zorgen dat persoonsgegevens, gelet op de doeleinden waarvoor ze worden verwerkt, juist en nauwkeurig zijn:

- fysieke maatregelen voor toegangsbeveiliging en logische toegangscontrole;
- opslag van gegevens in een kluis;
- project-, risico- en incidentenmanagement;
- data opsplitsen;
- dataminimalisatie;
- back-ups;
- integriteitscontroles;
- meerfactor-authenticatie;
- monitoring en logging;
- controle van toegekende bevoegdheden;
- privacybewustzijn- en beveiligingstrainingen;
- managementrapportages over risicobeheer;
- beperken inzageniveau;
- periodiek een audit of hack- of penetratietest uitvoeren;
- richtlijnen inzake gebruik ICT-hulpmiddelen, zoals versleutelde USB-sticks en beveiligde opslagplekken;
- responsible-disclosurebeleid;
- geheimhoudingsverklaringen;
- service level agreements (met boeteclausules);
- verwerkersovereenkomsten;
- screening personeel en VOG-verklaring.

Bij het bepalen van de gepaste maatregelen moet ook rekening gehouden worden met maatregelen die voortvloeien uit de Baseline Informatiebeveiliging Rijksdienst (BIR).

De Richtlijn noemt tot slot de volgende maatregelen:

- a. controle op de toegang tot de apparatuur;
- b. controle op de gegevensdragers;
- c. opslagcontrole;
- d. gebruikscntrole
- e. controle op de toegang tot gegevens;
- f. transmissiecontrole;
- g. invoercontrole;
- h. transportcontrole; en
- i. herstelbaarheid.

De Richtlijn verplicht tot het bijhouden van logbestanden van bepaalde vormen van verwerkingen, opdat het mogelijk is de reden, datum en het tijdstip van die handelingen te achterhalen en indien mogelijk de identiteit van de persoon die de persoonsgegevens heeft geraadpleegd of bekendgemaakt, en de identiteit van de ontvangers

van die persoonsgegevens.

Bij **conceptregelgeving**: ook op het niveau van regelgeving kunnen maatregelen worden getroffen. Denk hierbij aan het voorschrijven van maximum bewaartermijnen, het beperken van inzage in en besluiten over persoonsgegevens tot bepaalde functionarissen of geheimhoudingsverplichtingen.

Big Data

Bij Big data-analyses (zie punt 8) waarbij persoonsgegevens worden verwerkt, dient, gelet op de daarmee gepaard gaande risico's, in het bijzonder aandacht te worden besteed aan het treffen van de volgende maatregelen.

- Zorg ervoor dat naarmate de mogelijkheden van patroonherkenning bij de toepassing van big data minder zijn, een goede validatie door experts op het desbetreffende vakgebied plaatsvindt om het risico van foutieve uitkomsten zoveel mogelijk te reduceren.
- Zorg ervoor dat de data zoveel als met een redelijke inspanning mogelijk is, up to date zijn, de te gebruiken datasets een zo gering mogelijke bias (afwijking) bevatten en dat de te gebruiken algoritmen en analysemethoden deugdelijk zijn.
- Bepaal, rekening houdend met de potentiële impact van de toepassing, de foutmarge die bij de toepassing mag optreden.
- Zorg ervoor dat nuttige informatie aan betrokkenen wordt verschaft over de gebruikte logica achter de analyse en dat voor toezicht en rechterlijke toetsing voldoende inzicht kan worden gegeven in gebruikte algoritmen en analysemethoden.

Bij de toepassing van de uitkomsten van big data-analyses dient aandacht te worden besteed aan het treffen van de volgende maatregelen.

- Zorg voor menselijke tussenkomst in het proces van geautomatiseerde besluitvorming.
- Naarmate de potentiële negatieve impact voor de betrokkene groter wordt, neemt de noodzaak voor een goede validatie en een weging van de uitkomsten navenant toe.

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.



Bijlage Advies FG VWS PIA CoronaDashboard

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

1. Bronbestanden

- 2.
3. - Gegevensbeschermingseffectbeoordeling –PIA Coronadashboard Versie 3.0, d.d. 2 oktober 2020
- 4.

2. FG Advies

3.
 De Functionaris voor gegevensbescherming 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 effectbeoordeling - GEB, hierna te noemen PIA.

4. Uitgangspunten FG Advies

5.
 Bij de review van onderliggende PIA is uitgegaan van de privacy beginselen volgens de AVG en een zo laag mogelijke privacy risico voor de betrokkenen¹, 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 verwerkt.

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.

6.

7.

8. 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 de FG 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. De FG 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 authenticeren 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 FG

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.