1090242

Gegevensbeschermingseffectbeoordeling (PIA)

VWS, RIVM, CIb, EPI, RVP

CONTEST studie naar COVID-19 risicofactoren

Bilthoven, 7 december 2020

VWS, RIVM, CIb, EPI, RVP - CONTEST studie naar COVID-19 risicofactoren

Vaststelling verwerkersverantwoordelijke: 5 november 2020
Naam: 5.1.2e, 5.1.2e, 5.1.2e

Advies functionaris voor gegevensbescherming: 27 november 2020
Naam: 5.1.2e
Advies Privacy officer RIVM: 19 november 2020
Naam: 5.1.2e namens 5.1.2e
Advies CIO: 26 oktober 2020
Naam: 5.1.2e en 5.1.2e

Gegevensbeschermingseffectbeoordeling (PIA)

VWS, RIVM, CIb, EPI, RVP

CONTEST studie naar COVID-19 risicofactoren

Contact:

Ministerie van Volksgezondheid, Welzijn en Sport,
Parnassusplein 5
2511 VX Den Haag

Rijksinstituut voor Volksgezondheid en Milieu
Antonie van Leeuwenhoeklaan 9
3721 MA Bilthoven

Versie: 1.0

Inhoudsopgave

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.

Klik hier om infotekst te verbergen

Deze gegevensbeschermingseffectbeoordeling (PIA) is bedoeld voor de CONTEST studie naar COVID-19 risicofactoren, die wordt uitgevoerd door het centrum van Epidemiologie en Surveillance (EPI) van het RIVM. De aanleiding voor de CONTEST studie is de hoge besmettelijkheid en de gevolgen die een besmetting met SARS-CoV-2 op de gezondheid kan hebben.

Het doel van de studie is om inzicht te krijgen in de risicofactoren voor een SARS-CoV-2 infectie bij volwassenen die een SARS-CoV-2 test hebben gehad in een van de GGD teststraten in Nederland. De onderzoeksresultaten van deze studie kunnen helpen bij toekomstige teststrategieën, patiëntmanagement, volksgezondheidsmaatregelen en begeleiding en advies aan specifieke patiëntengroepen. Meer informatie over dit onderzoek is te vinden in het onderzoeksprotocol, welke als ***bijlage 1*** aan dit document is toegevoegd.

Sinds 6 april 2020 hebben 25 Gemeentelijke Gezondheidsdiensten (GGD'en) en Geneeskundige Hulpverleningsorganisaties in de Regio (GHOR) meer dan 80 COVID-19 "teststraten" in de buurt van een GGD of op een drive-in of drive-through locatie van de GGD ingericht. Van 6 april tot en met 31 mei 2020 richtte het testbeleid in de "teststraten" zich op specifieke risicogroepen. Vanaf 1 juni 2020 zijn de teststraten toegankelijk voor iedereen met COVID-19-achtige symptomen die zich vrijwillig wil laten testen.

Een persoon met COVID-19-achtige symptomen kan via het algemene telefoonnummer (0800-1202) of via coronatest.nl een afspraak maken voor een COVID-19 test in een van de teststraten. Het registratiesysteem van de teststraten, waarin de gegevens van degene die zich laten testen en de testuitslagen worden geregistreerd - genaamd CoronIT - wordt beheerd door GGD GHOR voor de GGD'en. De afspraak zal worden bevestigd door middel van een e-mail die vanuit CoronIT verstuurd wordt namens de GGD. In deze e-mail is een korte tekst en een link toegevoegd naar informatie over de CONTEST studie en de vragenlijst van de CONTEST studie (zie ***bijlage 2*** voorbeeld e-mail). Bij deze link staat vermeld dat enkel volwassenen mogen deelnemen aan de studie. Wanneer een potentiele deelnemer op de link klikt zal hij uit de e-mail omgeving gaan en geleid worden naar Formdesk. In Formdesk zal de deelnemer geïnformeerd

Om een PIA te kunnen verrichten moet duidelijk zijn op welk onderwerp/object deze betrekking heeft. Met een korte en bondige beschrijving van het voorstel waar de PIA op ziet, wordt tevens voorkomen dat bij het nalopen van de 17 punten hier verschillend over wordt gedacht. Ten behoeve van de duidelijkheid kan het nuttig zijn om expliciet aan te geven waar de PIA niet over gaat.Bij **conceptregelgeving** kan voor deze beschrijving van het voorstel aansluiting worden gezocht bij het voorlopige ontwerp van de inleidende paragraaf van de memorie of nota van toelichting bij het voorstel, voor zover deze betrekking heeft op verwerkingen van persoonsgegevens. Bij **overheidsverwerkingen** kan in hoofdlijnen worden beschreven hoe de gegevensverwerkingen er uit zullen zien. Als dat er is kan worden aangesloten bij het projectvoorstel of een beschrijving van de architectuur.

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.

ziektes en chronische aandoeningen

De complete vragenlijst van deze studie is te lezen in de bijlage toegevoegd aan deze PIA.

Daarnaast zullen de volgende laboratorium gegevens met betrekking tot de deelnemer zijn/haar COVID-19 test worden gedeeld met het RIVM:

- Laboratorium nummer (pseudoniem)
- Geboortejaar (persoonsgegevens)
- 4-cijferige postcode (persoonsgegevens)
- Datum test
- Soort test
- Teststraat van de afgenomen test
- Uitslag test

1. **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 persoonsgegeven. 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, relatiestatus 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, hartslag, 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, strafrechtketennummer 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;
- communicatieen 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 privacyregelgeving 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:

a. personen ten aanzien van wie gegronde vermoedens bestaan dat zij een strafbaar feit hebben gepleegd of zullen plegen;
b. personen die voor een strafbaar feit zijn veroordeeld;
c. 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
d. 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 **conceptregelgeving** 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.

- Sequence resultaten (niet van alle test

2. **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 persoonsgegeven. 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, relatiestatus 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, hartslag, 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, strafrechtketennummer 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;
- communicatieen 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 privacyregelgeving 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 ge'informeerd moet worden.
In het kader van de Richtlijn kan het onderscheid worden gemaakt tussen:

a. personen ten aanzien van wie gegronde vermoedens bestaan dat zij een strafbaar feit hebben gepleegd of zullen plegen;
b. personen die voor een strafbaar feit zijn veroordeeld;

c. 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
d. 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 **conceptregelgeving** 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.

De deelnemers van deze prospectieve studie betreffen volwassenen die zich op SARS-CoV-2 (hebben) laten testen in een GGD teststraat in Nederland. Om er zeker van te zijn dat enkel volwassenen deel nemen aan de studie, zijn er diverse checks ingebouwd (zie Onderdeel D: Maatregelen voor nadere informatie).

De deelnemers wordt gevraagd om specifieke persoons- en gezondheid gegevens in te vullen in een vragenlijst. Waarom persoonsgegevens van de deelnemers worden verzameld staat omschreven in paragraaf 14 'Noodzaak en evenredigheid'. Het betreft de volgende (categorieën) gegevens (zie ook ***Bijlage 4***):

Onderzoeksgegevens

- **Demografische gegevens:**
  - CoronIT nummer (pseudoniem)
  - Geboortejaar (algemeen)
  - Geslacht (algemeen)
  - 4-cijferige postcode (algemeen)
  - Geboorteland (bijzonder)
  - Geboorteland ouders (bijzonder)
  - Opleiding en beroep (algemeen)
  - E-mailadres (algemeen);
- **Gezondheidsgegevens (bijzonder):**
  - COVID-19 blootstelling gerelateerde gegevens, zoals:
    - gebruik van persoonlijke bescherming middelen,
    - houden aan COVID-19 gerelateerde maatregelen,
    - contact met geïnfecteerde personen,
    - bezoeken van openbare ruimtes zowel binnen als buiten,
    - bijwonen van activiteiten buitenshuis,
    - gebruik van openbaar vervoer,
    - en reizen.
  - COVID-19 gerelateerde symptomen;
  - Vaccinatiestatus en -datum (influenza, BCG, en later mogelijk ook COVID vaccinatie);
  - Zwangerschap;
  - Onderliggende ziektes en chronische aandoeningen.

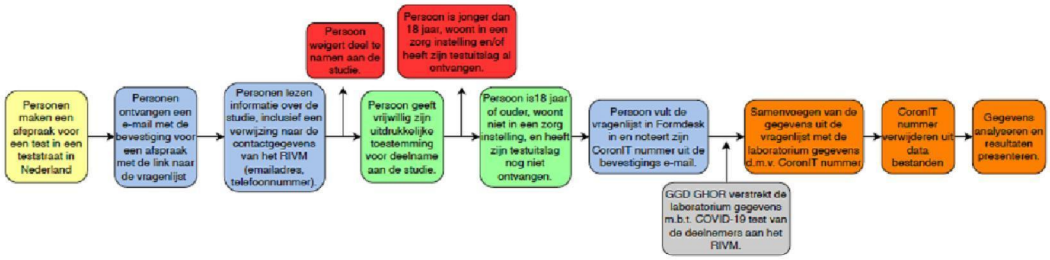
Daarnaast zal GGD GHOR bepaalde laboratoria gegevens met betrekking tot de SARS-CoV-2 test van de deelnemer delen met het RIVM. De wijze waarop deze gegevens verstrekt gaan worden staat uitgelegd onder Hoofdstuk 8 'Techniek en methode van gegevensverwerking'. Het betreft de volgende gegevens:

Laboratoriumgegevens:

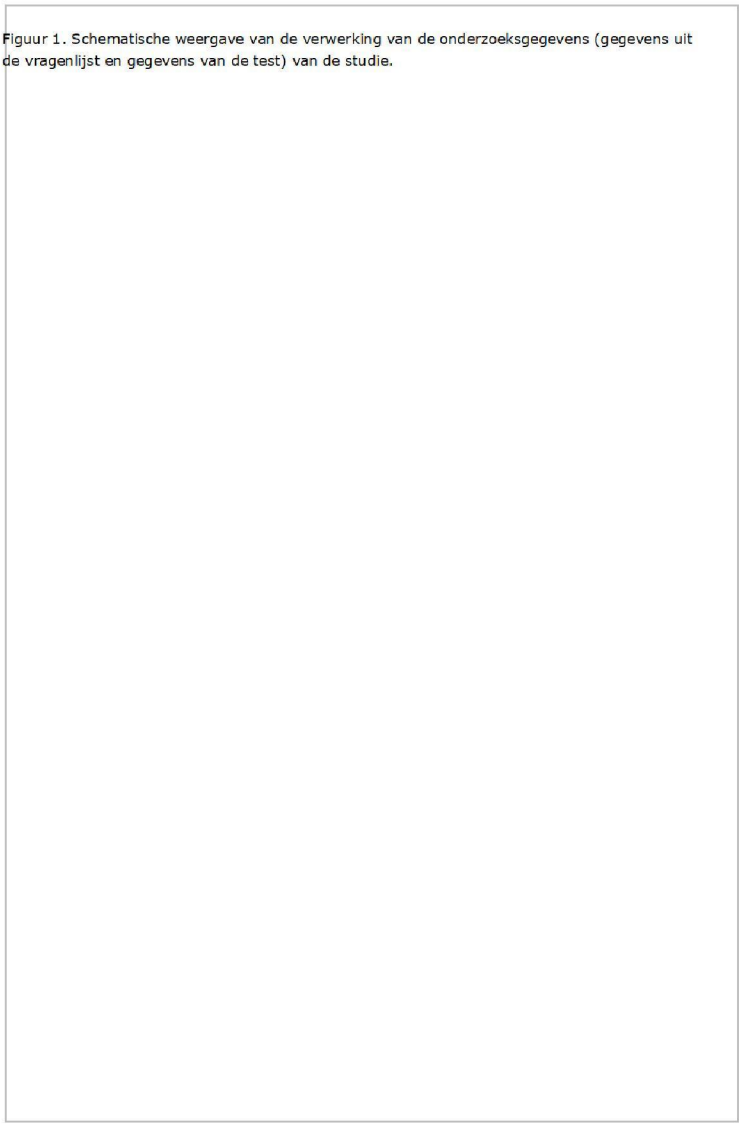
- CoronIT nummer (pseudoniem)
- Geboortejaar (algemeen)
- Geslacht (algemeen)
- 4-cijferige postcode (algemeen)
- Datum test (algemeen)
- Type test (bijzonder)
- Teststraat waar de test is afgenomen (algemeen)
- Uitslag test (bijzonder)

3. Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer.



totaal 3 keer onderwerp geweest van een penetratietest (uitgevoerd in opdracht van het RIVM), waarvan 2 zijn uitgevoerd na het datalek incident van een ander RIVM onderzoek Infectieradar. Hieruit zijn geen 'show stoppers' naar voren gekomen. Formdesk laat zelf ook regelmatig pentests uitvoeren op hun dienst. Daarnaast is er na het datalek incident bij Infectieradar opnieuw een uitgebreide risicoanalyse uitgevoerd, waarbij de conclusie was dat Formdesk als oplossing ingezet kan worden voor het ondersteunen van onderzoeken. De kwetsbaarheid (URL tampering) die ten grondslag lag aan het incident met Infectieradar kan niet meer voorkomen.
In de vragenlijst is ook een vraag opgenomen over het CoronIT nummer. Dit is een uniek nummer dat genoteerd staat in de bevestigingsmail die de deelnemers ontvangen van GGD GHOR. Nadat de deelnemer de vragenlijst heeft ingevuld en de testuitslag van de deelnemer bekend is, verstrekt GGD GHOR de laboratorium gegevens met betrekking tot de SARS-CoV-2 testuitslag van de deelnemers aan het RIVM via Zorgmail. De documenten worden opgeslagen op de servers van het RIVM (netwerkschijven). Vervolgens gaan de rechtstreeks betrokken onderzoekers van het RIVM het unieke CoronIT nummer, waarmee de gegevens uit de vragenlijst samengevoegd konden worden met de gegevens uit het laboratorium, vervangen door een studienummer (pseudonimisering). Het CoronIT nummer zal na de koppeling definitief verwijderd worden. Het document met CoronIT nummers zal tot de verwijdering enkel toegankelijk zijn met een wachtwoord en opgeslagen worden op een afgeschermde en beveiligde map op de netwerkschrijf van het RIVM. Na het uitvoeren van alle bovenstaande omschreven stappen, kunnen we de onderzoeksgegevens (gegevens uit de vragenlijst en gegevens over de test) analyseren en resultaten publiceren. Een verdere omschrijving



Figuur 1. Schematische weergave van de verwerking van de onderzoeksgegevens (gegevens uit de vragenlijst en gegevens van de test) van de studie.

3. Verwerkingsdoeleinden

3.

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 toegespitst 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 gedoeld 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 deze verwerkingen is het uitvoeren van wetenschappelijke onderzoek om de belangrijkste risicofactoren voor COVID-19 te onderzoeken. Dit doen we door gegevens te verzamelen (zie 2. Persoonsgegevens) van personen die de "teststraten" in Nederland bezoeken.

Ook worden separaat van dit onderzoek de emailadressen van betrokkenen bij het CONTEST onderzoek met hun toestemming gedurende 5 jaar bewaard met het oog op vervolgonderzoeken. Na afloop van deze vijf jaar worden ook deze gegevens door een betrokken onderzoeker van het RIVM vernietigd. De reden hiervoor is de verwachting dat onderzoeken omtrent COVID-19de komende jaren verder opgezet zullen worden. Deze bewaartermijn biedt de mogelijkheid om de deelnemers in het kader van vervolgonderzoek op het gebied van COVID-19 risicofactoren opnieuw te benaderen voor verbredend of verdiepend onderzoek.

De onderzoeksresultaten van deze studie kunnen helpen bij toekomstige teststrategieën, patiëntmanagement, volksgezondheidsmaatregelen en begeleiding en advies aan specifieke patiëntengroepen.

3. 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.

Klik hier om infotekst te verbergen

Om de rechtmatigheid van de voorgenomen gegevensverwerkingen te kunnen beoordelen, moet inzichtelijk zijn welke organisaties (functioneel) betrokken zijn bij welke gegevensverwerking en in welke hoedanigheid: verwerkingsverantwoordelijke, verwerker, verstrekker of ontvanger.

Verwerkingsverantwoordelijk is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan, die/dat het doel van en de middelen voor de gegevensverwerkingen vaststelt. Met andere woorden: degene die formeel bevoegd is te beslissen of persoonsgegevens worden verwerkt, voor welke doeleinden deze worden verwerkt en op welke wijze deze worden verwerkt. Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijke en moeten zij onderling vastleggen wie waarvoor verantwoordelijk en aansprakelijk is.

Verwerker is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. De verwerker verwerkt persoonsgegevens voor de verwerkingsverantwoordelijke, dat wil zeggen volgens diens instructies en onder diens verantwoordelijkheid. De verwerker is een buiten de organisatie van de verwerkingsverantwoordelijke staande persoon of organisatie. De verwerkingsverantwoordelijke en verwerker moeten onderling schriftelijk vastleggen wie waarvoor verantwoordelijk en aansprakelijk is. Om in een concreet geval te bepalen wie de verwerkingsverantwoordelijke is en wie de verwerker is, moet naast de formele taakverdeling zoals partijen die onderling hebben afgesproken ook worden gekeken naar de feitelijke omstandigheden (waarom vindt de verwerking plaats? Wie heeft deze geïnitieerd?). Dat betekent dat enkel het schriftelijk vastleggen van de taakverdeling niet voldoende is: ook in de praktijk moet de verwerkingsverantwoordelijke zeggenschap hebben over het doel en de middelen van gegevensverwerkingen.

Ontvanger is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan aan wie/waaraan de

persoonsgegevens worden verstrekt. Verstrekker is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan die/dat de persoonsgegevens ter beschikking stelt.

Bij **conceptregelgeving** kan het wenselijk zijn om daarin de hoedanigheid van de betrokken organisaties vast te leggen of volgens welke criteria deze wordt aangewezen. Indien een specifieke regeling over gegevensverwerkingen wordt opgesteld ten behoeve van een publiekrechtelijke taak, dient in de regeling de verwerkingsverantwoordelijke te worden aangewezen. Zo is in de Basisregistratie personen vastgelegd wanneer het college van burgemeester en wethouders en wanneer de minister verantwoordelijk is voor het bijhouden van persoonsgegevens in de basisregistratie. In bepaalde gevallen kan het ook wenselijk zijn om wettelijk voor te schrijven dat de toegang tot bepaalde persoonsgegevens beperkt blijft tot een specifieke functionaris, zoals een officier van justitie, vertrouwenspersoon of bedrijfsarts.

Bij **overheidsverwerkingen** zullen, voor zover niet reeds wettelijk voorgeschreven, de organisaties die (functioneel) betrokken zijn bij de gegevensverwerkingen zelf en in onderling overleg moeten bepalen wie in welke hoedanigheid de persoonsgegevens verwerkt. Tevens zal moeten worden bepaald, voor zover eveneens niet wettelijk voorgeschreven, welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens, bijvoorbeeld aan de hand van een autorisatiematrix, in relatie tot de doeleinden van de gegevensverwerking. Hierin kan tevens worden bepaald in welke gevallen en onder welke voorwaarden deze functionarissen toegang krijgen tot de persoonsgegevens.

RIVM
De verwerkersverantwoordelijke is het RIVM, deze stelt namelijk het doel en de middelen vast. De rechtstreeks betrokken onderzoekers van het RIVM coördineren de studie, bundelen de gegevens, voeren de analyses uit en hebben toegang tot de gekoppelde gegevens van de deelnemers.
Het RIVM is tevens ontvanger van persoonsgegevens die op haar verzoek door de GGD GHOR aan het RIVM worden verstrekt. Ook voor de verwerking van deze gegevens is het RIVM zelfstandig verwerkingsverantwoordelijke.

GGD GHOR
GGD GHOR Nederland is gezamenlijk verantwoordelijk met de GGD'en voor de gegevensverwerking in CoronIT. GGD GHOR Nederland heeft de opdracht van VWS gekregen en heeft het systeem ontwikkeld voor de GGD'en. Voor de taken van GGD GHOR Nederland is een convenant afgesloten. Enkel met de instemming van de GGD'en en beschreven taakverdeling in het convenant, heeft GGD GHOR Nederland de mogelijkheid gegevens te verwerken voor de GGD'en. De kwalificatie als gezamenlijk verantwoordelijke komt voort uit de grote rol die GGD GHOR Nederland heeft gekregen in het ontwikkelen van de applicatie. Hierover bestaat rechtspraak.

Deze uitwisseling is niet bepaald in het convenant, noch in de wet. Daarom is het van belang dat de GGD'en hierover een mening kunnen vormen en de opdracht verstrekken aan GGD GHOR Nederland om deze gegevens te verwerken. Alleen dan zal de DSA worden getekend. GGD GHOR vervult daarmee de rol van verstrekker. De DPG raad van GGD GHOR zal schriftelijk aangeven dat ze de laboratorium gegevens van de betrokkenen die uitdrukkelijke toestemming hebben gegeven mogen delen met het RIVM.

Bovenstaande tekst is opgesteld in samenspraak met 5.1.2e Privacy Lead van GGD GHOR.

Innovero (Formdesk)
Innovero is de leverancier van Formdesk. Met Innovero is een verwerkersovereenkomst afgesloten. In Formdesk vullen de deelnemers de vragenlijst in. Innovero verwerkt daarmee in opdracht van het RIVM persoonsgegevens ten behoeve van de CONTEST studie. Formdesk heeft, na het incident met de vorige versie van de Infectieradar, een negatieve bijklank. Analyse door de CISO RIVM van de actuele versie van Formdesk toont aan dat dit niet terecht is, en het advies aan de CISO RIVM is het gebruik van Formdesk wat betreft informatiebeveiliging te accorderen. De CISO RIVM heeft dit advies gevolgd (zie **Bijlage 5** en **Bijlage 8**).

Enovation BV (Zorgmail)
Voor de uitwisseling van persoonsgegevens tussen GGD GHOR en het RIVM wordt gebruik gemaakt van Zorgmail. Dit is een dienst die wordt aangeboden door het bedrijf Enovation (**Bijlage 5**). Deze dienst heeft zich inmiddels bewezen als een veilige methode om versleutelde e-mails te versturen. Veel zorgorganisaties en zorgverleners (denk aan zorginstellingen, ziekenhuizen en huisartsen) maken hier ondertussen gebruik van. Enovation is onder andere ISO 27001 en NEN7510 gecertificeerd. Er zal een bestand met Coronit-IDs naar GGD GHOR gestuurd worden via Zorgmail. GGD GHOR gebruikt deze IDs om te bepalen welke testuitslagen relevant zijn voor dit onderzoek.
Vanuit GGD GHOR zullen bestanden met de relevante testuitslagen via Zorgmail verstuurd worden naar het RIVM. Dit overzicht bevat de Coronit-IDs en de bijbehorende uitslag (positief of negatief voor SARS-CoV-2).
Zorgmail is hiermee een verwerker van het RIVM: zij verzorgt de veilige digitale uitwisseling van persoonsgegevens in opdracht van het RIVM.

Equinix
Het RIVM maakt voor de opslag van de gegevens gebruik van de data centers van Equinix te Amsterdam. Daarbij geldt dat de gegevens in principe binnen de EER blijven. Indien doorgifte naar een datacenter in een derde land nodig is, dan heeft Equinix Binding Corporate Rules (BCR's) die wereldwijd afdoende waarborgen bieden voor een passende bescherming van persoonsgegevens zoals dat door de AVG wordt vereist. Daarnaast beschikt Equinix over diverse certificeringen en past zij diverse internationale standaarden toe op het gebied van informatiebeveiliging.

4. Belangen bij de gegevensverwerking

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

Klik hier om infotekst te verbergen

Bij de beoordeling van de rechtmatigheid van de gegevensverwerkingen kunnen tevens de belangen (lees: de waarde of de voordelen) die met de gegevensverwerkingen gemoeid zijn een rol spelen. Het kan hierbij zowel gaan om de private belangen van de verwerkingsverantwoordelijke, betrokkene en derden als het algemeen belang. Het gaat hier dus niet om de (mogelijk) negatieve gevolgen voor de betrokkenen. Denk hierbij bijvoorbeeld aan: bedrijfsbelangen, financiële belangen en commerciële belangen, het handhaven van juridische vorderingen, toezicht op medewerkers ten behoeve van de veiligheid of managementdoeleinden, (nationale of openbare) veiligheid, zoals de preventie van fraude, misbruik en netwerkbeveiliging, en gezondheid.

Het belang dat gemoeid is met de gegevensverwerkingen werkt door in de toets van de noodzaak (zie punten 11 en 14 hierna).

De verwerkers, Innovero en Enovation, hebben als commerciële dienstverleners een algemeen commercieel belang bij gebruik van hun diensten. Dit belang is echter niet direct verbonden aan het onderhavige wetenschappelijke onderzoek.

Het algemene belang van dit onderzoek is om meer inzichten te krijgen in de risicofactoren van een SARS-CoV-2 infectie. Al eerder in deze PIA is benoemd dat het hierdoor mogelijk is om te helpen bij toekomstige teststrategieën, patiëntmanagement, volksgezondheidsmaatregelen en begeleiding en advies aan specifieke patiëntengroepen. GGD GHOR ziet belang bij de studie, omdat deze mogelijk kan helpen bij toekomstige test strategieën.

Het RIVM heeft als belang het bewaken en bevorderen van de volksgezondheid. Onderdeel hiervan vormt het onderzoeken van factoren die van invloed zijn op de voorkoming of bestrijding van ziekten in de Nederlandse samenleving. Deze belangen zijn onlosmakelijk verbonden met het doel en de kerntaken van het RIVM.

4. Verwerkingslocaties

Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

De verwerking van alle persoonsgegevens door betrokken partijen (zie onderdeel 6) vindt plaats in Nederland.

4. 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:

a. noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een

verwerkingsverantwoordelijke;

b. 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

c. 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:

a. wettelijk is toegestaan; en

b. 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.

Er is **geen** sprake van automatische besluitvorming, profilering of big data analyse zoals bedoeld in de AVG. Het onderzoek is namelijk niet gericht op het krijgen of bieden van inzichten ten behoeve van individuele deelnemers of groepen. Het geboorteland (van de ouders) wordt alleen gebruikt om de etnische achtergrond van de deelnemer te bepalen wat ook een mogelijke risicofactor is van COVID-19. Het is namelijk gebleken dat sommige ziekten, zoals diabetes en overgewicht, meer voorkomt bij bepaalde bevolkingsgroepen. Die aandoeningen maken mensen mogelijk extra kwetsbaar voor COVID-19 (Pareek et al., 2020; CBS, 2020).

Deelnemers vullen eenmalig de vragenlijst in via Formdesk. Eenmaal per dag zullen de resultaten vanuit Formdesk geëxporteerd worden naar een beveiligde folder op de R:\ schijf van het RIVM; na deze export worden de gegevens bij Formdesk gewist. Dit zal door een van de rechtstreeks betrokken onderzoekers gedaan worden. Vervolgens worden deze gegevens opgeslagen op een afgeschermde en beveiligde map op de netwerkschrijf van het RIVM. Deze map is enkel toegankelijk voor de betrokken onderzoekers (<10 onderzoekers). Zie Hoofdstuk 16 voor meer informatie over Formdesk.

De laboratoriumgegevens van GGD GHOR worden via Zorgmail beveiligd verzonden naar het RIVM. GGD GHOR zal de laboratorium gegevens verzenden naar een RIVM e-mailadres die specifiek is aangemaakt voor deze studie. De rechtstreeks betrokken onderzoekers (<10) hebben toegang tot deze mailbox. Vervolgens worden de gegevens uit de vragenlijst samengevoegd met de gegevens uit de testuitslag op basis van het CoronIT nummer. Dit gebeurt op de afgeschermde en beveiligde (twee-factor-authenticatie) netwerkschijf van het RIVM die alleen toegankelijk is voor de betrokken onderzoekers. Na deze koppeling wordt een studienummer aangemaakt en worden de CoronIT-nummers uit de databestanden definitief verwijderd. Zodoende staat in het databestand wat gebruikt wordt voor het analyseren van de data alleen het studienummer en niet het CoronIT nummer. Het databestand zal opgeslagen worden op de netwerkschijf van het RIVM in een map die alleen toegankelijk is voor de betrokken onderzoekers. De netwerkschijf is beveiligd met een twee-factor-authenticatie en daarnaast zal het bestand enkel te openen zijn door middel van een wachtwoord en encrypted zijn door gebruik te maken van 7-zip.

Van de deelnemers die hebben aangegeven in de toekomst benaderd te willen worden voor vervolgonderzoek is ook het e-mail adres bij ons bekend. Deze deelnemers hebben aan het eind van de vragenlijst hun e-mailadres ingevuld in Formdesk. Dit e-mailadres zal na het exporteren van de gegevens uit Formdesk direct worden opgeslagen in een ander bestand. Het bestand met deze e-mailadressen zal worden opgeslagen op de netwerkschijf van het RIVM in een map (anders dan de map waar de overige onderzoeksgegevens in opgeslagen zijn) die alleen toegankelijk is voor de rechtstreeks betrokken onderzoekers. De netwerkschijf is beveiligd met een twee-factor-authenticatie en het bestand met de e-mailadressen zal enkel te openen zijn door middel van een wachtwoord en encrypted zijn door gebruik te maken van 7-zip.

4. 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.

Klik hier om infotekst te verbergen

Naast of in de plaats van de AVG en de Richtlijn kan (sectorale) regelgeving de mogelijkheden voor gegevensverwerkingen creëren, conditioneren of beperken. Voorbeelden van dergelijke wetten zijn: Wet algemene bepalingen burgerservicenummer, Wet gebruik burgerservicenummer in de zorg, Wet basisregistratie

personen, Algemene wet inzake rijksbelastingen, Archiefwet, Telecommunicatiewet, Kadasterwet, Handelsregisterwet 2007, Kieswet, Wet bijzondere maatregelen grootstedelijke problematiek, Wet op de geneeskundige behandelingsovereenkomst, Omgevingswet, Jeugdwet, Wet maatschappelijke ondersteuning 2015 en Participatiewet. Deze lijst is niet uitputtend.

Er kan ook departementaal of rijksbreed beleid zijn dat de mogelijkheden voor de voorgenomen gegevensverwerkingen conditioneert of beperkt. Bijvoorbeeld ten aanzien van de opslag en beveiliging van persoonsgegevens.

Aan de hand van deze inventarisatie kan bij onderdeel B beoordeeld worden of de voorgenomen gegevensverwerkingen rechtmatig zijn en bij onderdeel D of specifieke maatregelen voorgeschreven zijn.

De volgende wetten en regelgeving zijn relevant voor het verwerken van persoonsgegevens in dit onderzoek:

- Wet publieke gezondheid;
- Besluit publieke gezondheid;
- De Wet op het RIVM (artikel 3, lid 1, sub a);
- Wet medisch-wetenschappelijk onderzoek met mensen (o.a. Artikel 1);
- Niet-WMO verklaring van het KEC;
- Uitvoeringswet AVG;
- Archiefwet;
- Selectielijst RIVM 2004 – (Staatscourant Nr. 20886, april 2017).

4. 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

Op grond van de Archiefwet heeft het RIVM een selectielijst, getiteld "Selectielijst RIVM 2004..." (voortaan: de selectielijst). In deze selectielijst staat een overzicht van processen die bij het RIVM gebeuren met daaraan gekoppeld de wettelijke bewaartermijnen.

De gegevens die in het kader van de huidige studie worden verzameld hebben regulier een bewaartermijn van 10 jaar op basis van de selectielijst. Het verzamelen van deze gegevens valt onder categorie 4.5 van de selectielijst. Echter, op dit moment valt het huidige onderzoek met haar doelstellingen onder het bereik van de rijksbrede hotspot. Dit houdt in dat de documentaire neerslag van deze crisis, waaronder (niet uitputtend) documenten, databases, e-mails, websites en uitingen op sociale media blijvend te bewaren zijn.

Bij de verzameling van persoonsgegevens dient ook rekening te worden met de AVG en de archiefwet. (De duur van) Bewaring van persoonsgegevens in de database is hierbij afhankelijk van ondermeer de rechtsgrond voor bewaring en de doelstelling waarmee de persoonsgegevens worden bewaard. In de kern dient een afweging is tussen enerzijds de privacybelangen van de betrokkenen bij het onderzoek op grond van de AVG en anderzijds de cultuur-historische belangen vanuit de archiefwet te worden gemaakt. Voor databases met persoonsgegevens die worden bewaard onder de rechtsgrond "toestemming van de betrokkene" is door de DG van het RIVM met instemming van de FG van het ministerie van VWS bepaald dat deze geanonimiseerd opgeslagen worden. Voor deze geanonimiseerde dataset geldt bewaartermijn: blijvend (B).

Los van de database die wordt opgezet in het kader van het huidige onderzoek wordt een verzameling emailadressen bijgehouden van deelnemers die aan vervolgonderzoek willen deelnemen. Deze mailadressen worden vijf jaar bewaard. Deze bewaartermijn biedt de mogelijkheid om de deelnemers in het kader van vervolgonderzoek op het gebied van COVID-19 risicofactoren opnieuw te benaderen voor verbredend of verdiepend onderzoek.

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.

5. 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.

Deelname aan het onderzoek is vrijwillig. De betrokkene moet dus zelf uitdrukkelijke toestemming geven voor de verwerking van de gegevens uit de vragenlijst. Daarnaast moet de betrokkene ook toestemming geven aan GGD GHOR om de gegevens van de labuitslagen met het RIVM te delen. (6.1.a AVG) (6.1.e AVG).

De persoonsgegevens die worden verzameld voor vervolgonderzoek hebben de grondslag:

- Art. 6.1.a AVG: geïnformeerde toestemming van betrokkenen

5. 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.

Klik hier om infotekst te verbergen

De AVG verbiedt de verwerking van bijzondere persoonsgegevens. Op dit verwerkingsverbod gelden de volgende uitzonderingen:

a. de betrokkene heeft uitdrukkelijke toestemming gegeven;
b. de verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten op het gebied van arbeids- en sociaalzekerheidsrecht;
c. de verwerking is noodzakelijk ter bescherming van vitale belangen van de betrokkenen of een ander;
d. de verwerking wordt verricht door een instantie die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is;
e. de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn

gemaakt;
f. de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
g. de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang;
h. de verwerking noodzakelijk is voor preventieve en arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid, medische diagnosen, het verstrekken van gezondheidzorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en –diensten of sociale stelsel en diensten;
i. de verwerking noodzakelijk is om redenen van algemeen belang op het gebied van de volksgezondheid;
j. de verwerking noodzakelijk is met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.

Verdere uitzonderingen zijn te vinden in nationale regelgeving.

De AVG bepaalt daarnaast dat verwerking van strafrechtelijke gegevens alleen is toegestaan door of onder toezicht van de overheid of als dit bij wet geregeld is (zie voor de definitie van strafrechtelijke gegevens de toelichting bij punt 2).

De verwerking van nationale identificatienummers is alleen toegestaan ter uitvoering van de wet of voor doeleinden die bij wet zijn bepaald. Overheidsorganen kunnen bij de uitvoering van hun publieke taak gebruik maken van het burgerservicenummer, zonder dat daarvoor nadere regelgeving vereist is.

De Richtlijn schrijft voor dat verwerking van bijzondere persoonsgegevens slechts is toegestaan wanneer de verwerking strikt noodzakelijk is, geschiedt met inachtneming van passende waarborgen voor de rechten en vrijheden van betrokkene, en:
a. wettelijk is toegestaan;
b. noodzakelijk is om vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen; of
c. die verwerking betrekking heeft op gegevens die kennelijk door de betrokkene zelf openbaar zijn gemaakt.

Bij **conceptregelgeving** kan van het verbod op de verwerking van bijzondere of strafrechtelijke persoonsgegevens worden afgeweken, mits passende waarborgen worden geboden ter bescherming van persoonsgegevens en andere grondrechten van de betrokkene.

Voor het doel van het onderzoek is de verwerking van persoonsgegevens noodzakelijk. Onder deze persoonsgegevens vallen tevens bijzondere persoonsgegevens, namelijk gegevens over gezondheid waarvoor in beginsel een verbod op verwerking geldt. Op de verwerkingen in het kader van dit onderzoek is de uitzondering ex art. 9.2.i AVG van toepassing. Er is sprake van:
- een grond in Unierecht of lidstatelijk recht (artikel 3 Wet op het RIVM en artikel 6c Wpg);
- waarin passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van de betrokkene (de pseudonimiseringsplicht in artikel 6c.3 Wpg en het beroepsgeheim in art. 7:457 BW en artikel 88 Wet BIG).

6. 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.

De persoonsgegevens worden verzameld voor het doeleinde van deze studie, zoals beschreven in onderdeel 4. Gegevens verzameld binnen de studie worden dus niet anders verwerkt dan voor het specifieke doel waarvoor bedoeld (volgens protocol) en waarover is gecommuniceerd met de deelnemers.

Hoewel niet de verantwoordelijkheid van het RIVM, geldt wat betreft de verstrekking van gegevens door GGD GHOR het volgende. GGD GHOR verstrekt gegevens die oorspronkelijk voor een ander doeleinde zijn verzameld dan die verstrekking. De AVG geeft hier ruimte voor als die verstrekking niet onverenigbaar is met het doeleinde waarvoor de gegevens oorspronkelijk zijn verzameld.

Op grond van artikel 5.1.b AVG geldt het verder verwerken van persoonsgegevens in het kader van wetenschappelijk onderzoek als niet onverenigbaar, als die verwerking conform artikel 89 lid 1 AVG geschiedt. Twee belangrijke waarborgen hier zijn dat de gegevens alleen worden verstrekt als de betrokkene op vrijwillige basis toestemming geeft, en het feit dat de gegevens in gepseudonimiseerde vorm worden verstrekt.

6. Noodzaak en evenredigheid

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

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

Het doel van deze verwerkingen is het uitvoeren van wetenschappelijke onderzoek om de belangrijkste risicofactoren voor COVID-19 te onderzoeken. Hieronder wordt de proportionaliteit en de subsidiariteit beoordeeld.

De huidige gegevensverwerking zijn **proportioneel** omdat:

1. De verwerking van de gegevens essentieel is voor het uitvoeren van dit onderzoek. De gegevens worden door deelnemers op basis van uitdrukkelijke toestemming verstrekt voor de verwerking van de gegevens uit de vragenlijst, voor de gegevens verstrekt door GGD GHOR, en voor de verwerking van de emailadressen, nadat zij hierover conform de voorwaarden in de AVG geïnformeerd zijn;
2. Er slechts gegevens verzameld worden die noodzakelijk zijn voor de uitvoering van het onderzoek en haar doelstellingen. Waar mogelijk wordt dataminimalisatie toegepast of gebruik gemaakt van pseudoniemen;
3. Vanwege de vergelijking van positief en negatief geteste personen, en de persoonlijke aard van de gegevens, zoals symptomen, is er geen andere manier om zo de hieraan verbonden ernstige gevolgen voor de volksgezondheid en staat van de Nederlandse economie te beperken, en er geen andere manier is om aan voldoende van dit soort gegevens te komen.

- kan bij het gebruik van bijzondere of strafrechtelijke persoonsgegevens hetzelfde resultaat behaald worden met gebruikmaking van een combinatie van gewone persoonsgegevens?
- kan het verwerken van de persoonsgegevens in een beperktere vorm of met minder verwerkingen?

Zo kan in bepaalde gevallen met foto's hetzelfde doel worden bereikt (bijvoorbeeld: identificatie) als met het verwerken van filmbeelden. Het subsidiariteitsbeginsel houdt bijvoorbeeld ook in dat als persoonsgegevens openbaar gemaakt gaan worden, niet automatisch alle persoonsgegevens openbaar worden gemaakt, maar een selectie wordt gemaakt op grond van gerechtvaardigde criteria. Bij deze afwegingen worden de doelen, belangen en feiten zoals in beeld gebracht in onderdeel A betrokken.

Bij **conceptregelgeving** kunnen de uitkomsten van deze afweging worden meegenomen in de grondrechtentoets van het IAK.

Daarnaast is bij de gegevensverwerking sprake van **subsidiariteit**, omdat:

1. Zonder deze gegevens kunnen de doelstellingen niet bereikt worden;
    a. Het onderzoek zoals beschreven in deze PIA kan niet haar doelen behalen wanneer minder gegevens verzameld worden. Indien een onderzoek met minder gegevens wordt uitgevoerd, is de waarde van de resultaten minder omdat het geen compleet beeld geeft van de relevante risicofactoren. Bij de opzet van een studie wordt altijd goed nagedacht over welke data nodig zijn voor een zinnig onderzoek. De uitkomst is de onderzoeksopzet.
    b. De gegevens worden gepseudonimiseerd door middel van definitieve verwijdering van het CoronIT nummer nadat de koppeling van de gegevens uit de vragenlijst met de laboratoriumgegevens plaats heeft gevonden. Veel verder dan dat kan het niet gaan, omdat er een koppelmethode nodig is die de labuitslagen en vragenlijst bij elkaar houdt.
2. Deze gegevens niet op een andere, minder ingrijpende wijze verzameld kunnen worden. De deelnemer wordt eenmalig uitgenodigd, en hoeft in het kader van de CONTEST studie ook maar eenmalig de vragenlijst in te vullen. De controle over het wel of niet beschikbaar stellen van de gegevens ligt bij de deelnemer. Het doel kan daarmee niet op een minder ingrijpende wijze gerealiseerd worden.
    a. De manier van betrokkenen benaderen kan anders, bijvoorbeeld via steekproefsgewijze CBS-uittreksels, maar daarmee verwerk je juist meer gegevens van betrokkenen die niet relevant zijn, bijvoorbeeld omdat ze zich niet hebben laten testen. Daarnaast ontvangen mensen dan een gericht verzoek om mee te doen aan een onderzoek, wat als ingrijpender kan worden ervaren dan een standaard uitnodiging die deel uitmaakt van een afspraakbevestiging.
3. Om te checken of deelnemers het goede CoronIT nummer hebben ingevuld controleert GGD GHOR of het geboortejaar, geslacht en 4-cijferige postcode dat de deelnemer heeft ingevuld in de vragenlijst correspondeert met die gegevens in CoronIT. Op deze manier wordt gecontroleerd of de testuitslag correspondeert met dezelfde persoon die de vragenlijst heeft ingevuld.
4. Het geboortejaar zal gebruikt worden om de leeftijd van een deelnemer te berekenen. Leeftijd en geslacht zijn belangrijke risicofactoren van COVID-19 en zijn daarom in het bijzonder van belang voor deze studie.
5. De 4-cijferige postcode hebben we nodig om een indruk te krijgen van de Sociaal Economische Status (SES) van de deelnemers. Het geboorteland (van de ouders) willen we gebruiken om de etnische achtergrond van de deelnemer te bepalen wat ook een mogelijke risicofactor kan zijn van COVID-19. Zo is gebleken dat sommige ziekten, zoals

diabetes en overgewicht, meer voor komt bij bepaalde bevolkingsgroepen. Die aandoeningen maken mensen mogelijk extra kwetsbaar voor COVID-19 (Pareek et al., 2020; CBS, 2020). Deelnemers zijn niet verplicht om hun geboorteland en het geboorteland van de ouders in te vullen.

6. Gegevens over de deelnemers hun beroep hebben we nodig, omdat bepaalde beroepen vaker bloot worden gesteld aan grote aantallen mensen, dit is bijvoorbeeld het geval bij beroepen in de gezondheidszorg. Hierbij is de kans aanwezig dat een persoon sneller in aanraking komt met een persoon positief voor COVID-19 dan dat het geval is bij het uitoefenen van een ander beroep. Daarom is het belangrijk om het beroep van de deelnemers te weten, wat een mogelijk risicofactor is voor het krijgen van COVID-19. Deelnemers zijn niet verplicht om gegevens over hun beroep in te vullen.
7. Het opleidingsniveau van de deelnemers willen we verzamelen, omdat we een indruk willen krijgen van de representativiteit van onze onderzoekspopulatie. Daarnaast is het opleidingsniveau onderdeel van sociaal economische status, wat ook een risicofactor kan zijn. Deelnemers zijn niet verplicht om het opleidingsniveau in te vullen.
8. Vaccinatiestatus en -datum hebben we nodig omdat dit mogelijk van invloed is op de COVID-19 gerelateerde symptomen.
9. De laboratoriumgegevens zijn noodzakelijk om vast te stellen of er daadwerkelijk sprake is van een besmetting met COVID-19, te controleren of deze gegevens corresponderen met de deelnemer en om te bepalen in welk postcodegebied deelnemers zich hebben laten testen.
10. Het unieke CoronIT nummer gaan we na koppeling van de vragenlijst en de testuitslag definitief verwijderen.
11. Archivering van de gegevens in kwestie vindt gepseudonimiseerd, geanonimiseerd plaats en wel zodanig dat de gegevens die worden gearchiveerd en op termijn overgedragen aan het Nationaal Archief niet meer herleidbaar zijn naar de betrokkenen die het betreft.

Geconcludeerd kan worden dat de verwerkingen in het kader van dit onderzoek beperkt zijn tot persoonsgegevens die noodzakelijk zijn voor de uitvoering van het onderzoek, de belangen van deelnemers niet onevenredig schaden en niet op een minder ingrijpende wijze verkregen kunnen worden.

7. 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:

a. de verwerkingsdoeleinden;
b. de categorieën van persoonsgegevens;
c. 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.

Het RIVM werkt met twee datasets. De eerste is het mailadressenbestand van mensen die bereid zijn in een later stadium voor vervolgonderzoek benaderd te worden. De tweede is het inhoudelijke gegevensbestand van labuitslagen en vragenlijsten. De twee gegevenssets zijn niet gekoppeld op basis van het CoronIT nummer. Wel zal op basis van het studienummer een link blijven met het emailadres en de vragenlijst. Het document met e-mailadressen valt buiten de reikwijdte van deze PIA en dus ook van dit onderdeel, omdat de emailadressen zijn verzameld voor een doel (namelijk het later benaderen voor onderzoeken).

Toepasselijkheid AVG-rechten in het kader van identificeerbaarheid betrokkenen

Het RIVM verwerkt (conform art. 6c Wpg) alleen gespeudonimiseerde persoonsgegevens. Het RIVM verwerkt in deze studie geen naam/toenaam, telefoonnummer, woonadres of andere direct herleidbare gegevens. Omdat de gegevensset indirect wel herleidbaar is (bijvoorbeeld in combinatie met de dataset bij GGD GHOR of omdat ingevulde antwoorden op de vragenlijsten potentieel tot spontane herleiding kunnen leiden) gaan we ervan uit dat er sprake is van persoonsgegevens en dat de AVG van toepassing is.

Voorafgaand aan de verwijdering van het bestand met CoronIT nummers hebben betrokkenen nog de mogelijkheid om hun gegevens te laten verwijderen. Op dat moment is er nog de mogelijkheid om de gegevens uit de vragenlijst te koppelen aan een CoronIT nummer. Na de verwijdering van het bestand met CoronIT nummers, kan het RIVM betrokkenen echter niet identificeren aan de hand van de dataset. De betrokkenen worden in de privacy verklaring (**Bijlage 9**) geïnformeerd over de identificatie met hun CoronIT nummer indien ze beroep willen doen op hun rechten. Als iemand zich met naam en toenaam, met andere direct identificerende gegevens of zelfs met BSN meldt om rechten uit te oefenen, is er voor het RIVM geen mogelijkheid om vast te stellen welke vragenlijst bij de betreffende persoon hoort. Het RIVM hoeft conform artikel 11.1 AVG geen gegevens bij te houden om identificatie mogelijk te maken (sterker nog, dat zou tegenstrijdig zijn met de plichten en maatregelen uit de Wpg en AVG). Als iemand rechten wil uitoefenen en het RIVM kan die persoon niet identificeren, dan zijn de artikelen 15-20 AVG niet van toepassing (art. 11.2 AVG) en kan het RIVM dus geen uitvoering geven aan de rechten van de betrokkene.

Ook als iemand aanvullende gegevens aanlevert (bijvoorbeeld antwoorden op de vragenlijst zoals postcode, geboorteland, geboorteland ouders, leeftijd), kan het RIVM niet vaststellen of die persoon daadwerkelijk de betrokkene is. Het kan ook een 'phishing expedition' zijn van bijvoorbeeld een buurman die de demografische gegevens van zijn buren kent en wil achterhalen of mensen om hem heen positief getest zijn op corona door inzageverzoeken in te dienen.

Het RIVM beschouwt artikel 15-20 AVG dan ook niet van toepassing in het kader van dit onderzoek.

In het theoretische geval dat iemand zulke gegevens aanlevert dat identificatie wél mogelijk is, gelden de volgende beperkingen.

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.

8. 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.

De verwerkingen hebben niet tot doel enige directe impact op betrokkenen te hebben. De betrokkenen hebben geen direct belang bij de resultaten van het onderzoek en ondervinden ook geen direct gevolgen van de uitslagen van het onderzoek. In die zin hebben de gegevensverwerkingen in het kader van dit onderzoek dan ook geen impact op betrokkenen als er niets fout gaat (zie daarover algemene risico's hieronder).

De kans bestaat wel dat betrokkenen indirect gevolgen ondervinden aan dit onderzoek, bijvoorbeeld als het onderzoek bepaalde risicofactoren in kaart brengt, waar vervolgens actief of preventief beleid op wordt gevoerd door de overheid. Ten eerste valt die mogelijkheid buiten de scope van deze PIA, omdat het geen gevolg is van de gegevensverwerking, maar het beleid dat erop volgt, en ten tweede stemmen personen zelf in met deelname aan het onderzoek. Het is wel relevant om te benoemen dat het onderzoek kan bijdragen aan onterechte negatieve impact op betrokkenen, als er met foutieve gegevens wordt gewerkt of er onterechte conclusies worden getrokken. De kans dat deze impact ontstaat is klein, omdat het een onwaarschijnlijke samenloop van verschillende omstandigheden vergt en omdat het RIVM maatregelen neemt om juiste gegevens op de juiste wijze te verwerken.

Algemene risico's
Los van de risico's per processtap geldt voor elke processtap een aantal 'standaard' risico's die zich kunnen voltrekken als men niet volgens de wettelijke kaders en RIVM-protocollen werkt. Voorbeelden zijn beveiligingsincidenten/datalekken, bewaartermijnoverschrijdingen, onrechtmatige verdere verwerking van persoonsgegevens. Die risico's zijn inherent aan elke gegevensverwerking en dus elke processtap.

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.

Risico's per processtap

***1.* Toestemming geven voor deelname aan het onderzoek**

Deelnemers zullen uitdrukkelijke toestemming moeten geven voor de verwerking van de gegevens uit de vragenlijst Daarnaast zal er ook uitdrukkelijke toestemming moeten worden gegeven zodat GGD GHOR de laboratorium uitslagen en andere gezondheidsgegevens met het RIVM mag delen. Indien de deelnemer niet zijn of haar toestemming geeft voor de bovenstaande omschreven doelen, kan het onderzoek geen doorgang vinden bij deze betrokkene. De deelnemer zal dan niet naar de vragenlijst worden geleid en bedankt worden. Dit is een risico op de verwerking.

2. Gebruiksgegevens in Formdesk omgeving vóór invullen vragenlijst

We kunnen geen noemenswaardige negatieve impact bedenken die voor betrokkenen kan volgen uit het verwerken van gebruiksgegevens in Formdesk door het RIVM. Gebruiksgegevens zoals IP-adres, sessietijd of cookiegegevens verwerkt het RIVM zelf niet via Formdesk. Formdesk doet dit als partij wel, en dat is om hun diensten te kunnen aanbieden. Deze gegevens worden echter niet doorgezet naar RIVM. De gegevens worden na maximaal 1 maand automatisch verwijderd uit

Formdesk.

3. Invullen vragenlijst in Formdesk

We kunnen geen noemenswaardige negatieve impact bedenken voor betrokkenen kan volgen uit het verwerken van gebruiksgegevens in Formdesk door het RIVM. De opslag van deze gegevens vindt plaats bij Formdesk en niet lokaal bij het RIVM. Het kan voorkomen dat iemand ervoor kiest om deel te nemen aan het onderzoek, spijt krijgt en niet meer wil deelnemen. Als de persoon tijdens het invullen van de vragenlijst besluit toch niet verder mee te willen doen, en de persoon uit de online omgeving van Formdesk gaat alvorens hij de vragenlijst heeft verzonden, zullen de gegevens niet opgeslagen worden op de servers van Formdesk. De persoon kan na verzenden zelf niet meer bij het vragenformulier, en het is ook praktisch onmogelijk om rechten zoals het recht op wissing uit te oefenen. In zekere zin verliest diegene dus controle over persoonsgegevens.

In principe biedt de AVG ook uitkomst in dezen, omdat de betrokkene de toestemming voor het delen van labuitslag nog kan intrekken als diegene op tijd is.

Daarnaast bestaat er een potentieel risico dat een select groepje databasebeheerders van Innovero (aanbieder Formdesk) in theorie toegang kunnen hebben tot de RIVM gegevens in de betreffende databases (zie **bijlage 5** voor analyse informatiebeveiliging). Met Innovero is een verwerkersovereenkomst afgesloten.

Verder kan een inbreuk op de persoonlijke levenssfeer (of vergelijkbare inbreuken) van één of meerdere betrokkenen optreden doordat de binnen de verwerking geregistreerde persoonsgegevens worden misbruik door een gebruiker, beheerder of leverancier.

Daarnaast is het mogelijk dat een datalek binnen de verwerking niet wordt gesignaleerd. Als gevolg daarvan kan het datalek voortduren en worden er geen maatregelen genomen om het datalek te dichten en om de gevolgen van het datalek te beperken. Dit is een potentieel risico binnen de verwerking van de gegevens in formdesk. Daarnaast zou het in theorie mogelijk kunnen zijn dat oneigenlijke toegang tot de gegevens niet wordt gedetecteerd.

Indien een deelnemer toestemming geeft aan het RIVM om in de toekomst benaderd te mogen voor vervolgonderzoek op het gebied van COVID-19, vult degene zijn/haar e-mailadres in. Op dat moment staat in Formdesk de ingevulde gegevens uit de vragenlijst en de e-mailadres van de deelnemers. Na het exporteren van deze gegevens uit Formdesk worden de gegevens afzonderlijk opgeslagen op de netwerkschijf van het RIVM. Deze gegevens worden na maximaal 1 maand automatisch verwijderd uit Formdesk. Er bestaat dus een tijdelijk risico (1 maand) dat de gegevens gezamenlijk opgeslagen staan in Formdesk. In theorie zou een select groepje databasebeheerders van Innovero (aanbieder Formdesk) toegang kunnen hebben tot deze gegevens (zie **bijlage 5** voor analyse informatiebeveiliging). Zoals eerder geschreven, met Innovero is een verwerkersovereenkomst afgesloten.

4. Verstrekken CoronIT nummers aan GGD GHOR voor labuitslagen (en ontvangen gegevens vanuit GGD GHOR)

In deze processtap bestaat de kans dat een betrokkene die een test afneemt controle verliest over persoonsgegevens en dat het medisch beroepsgeheim ten aanzien van die betrokkene onterecht wordt doorbroken. Dit kan gebeuren als het RIVM de verkeerde CoronIT-nummers uitvraagt. Omdat RIVM de nummers uit Formdesk exporteert, kan dit alleen voorkomen als deelnemers zelf een verkeerd CoronIT nummer invoeren. Maar GGD GHOR zal een check

uitvoeren op geboortejaar, geslacht, en postcode van de CoronIT nummers en dit document beveiligd naar ons mailen via Zorgmail. Indien het geboortejaar, geslacht en 4-cijferige postcode dat de deelnemer heeft ingevuld in de vragenlijst niet correspondeert met die gegevens in CoronIT, zal deelnemer geëxcludeerd worden uit het huidig onderzoek. De gegevens van de betreffende deelnemer zal dan verwijderd worden uit onze bestanden.

Mocht dit voorkomen, dan heeft dit geen direct merkbare impact op de betrokkene. Betrokkenen krijgen geen bevestiging of ander bericht dat hun gegevens zijn opgevraagd bij en verstrekt door GGD GHOR. Daarnaast wordt dan hun labuitslag gekoppeld aan een vragenlijst die ze niet hebben ingevuld, wat de kans op spontane herleiding stevig verkleint.

Mocht echter uitkomen dat dergelijke vergissingen bestaan, bijvoorbeeld omdat het wordt ontdekt en lekt naar de pers, kan de nieuwsverslaggeving hieromtrent een gevoel van onbehagen oproepen bij personen die een test hebben laten doen.

5. Samenvoegen laboratorium uitslagen en vragenlijsten
We kunnen geen noemenswaardige negatieve impact bedenken die voor betrokkenen kan volgen uit het samenvoegen van de laboratorium uitslagen met de gegevens uit de vragenlijsten.

6. Pseudonimisering
Zodra deze gegevens zijn samengevoegd zoals beschreven onder stap 5, verwijderen we het unieke CoronIT nummer definitief uit onze bestanden. Daarmee is de koppeling ook weg. Een mogelijk negatieve impact van de pseudonimisering van de gegevens, is dat na de koppeling en daarmee de verwijdering van het CoronIT nummer, deelnemers niet meer beroep kunnen doen op hun rechten. Voorafgaand aan de koppeling kunnen deelnemers dit nog wel.

6. Analyses
We kunnen geen noemenswaardige negatieve impact bedenken die voor betrokkenen kan volgen uit het analyseren van de data.

Zoals hierboven beschreven kunnen foutieve analyses of verkeerd onderbouwde conclusies wel indirecte gevolgen hebben, die zowel de betrokkenen als andere burgers kunnen raken. Omdat die impact niet uit deze gegevensverwerking volgt beschouwen we die impact als buiten de reikwijdte van deze PIA.

7. Archivering
We kunnen geen noemenswaardige negatieve impact bedenken voor betrokkenen kan volgen uit het archivering van de onderzoeksgegevens met het permanente bewaartermijn. Dit omdat de gegevens zonder herleidbare persoonsgegevens worden gearchiveerd. De bewaartermijn voor persoonsgegevens voor vervolgonderzoeken is doelbewust gelimiteerd tot 5 jaar. Na afloop hiervan worden deze gegevens conform het bepaalde in het Archiefbesluit 1995 vernietigd.

D. Beschrijving voorgenomen maatregelen

In onderdeel D wordt bezien welke maatregelen kunnen worden getroffen om de in onderdeel C erkende risico's te voorkomen of te verminderen. Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de wetgever of verwerkingsverantwoordelijke. Voor dit onderdeel van de PIA is, als het gaat om beveiligingsmaatregelen, expertise over informatiebeveiliging belangrijk.

9. 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.

bijvoorbeeld aan: het extra informeren van de betrokkenen, een extra keuze-, inspraak- of bezwaarmogelijkheid

Per processtap worden verschillende maatregelen genomen om verschillende risico's te mitigeren. De maatregelen staan hieronder opgesomd, met tussen haakjes het risico dat ze mitigeren. De risico's:
- Verlies controle persoonsgegevens (**VC**)
- Verkeerde koppeling labuitslag en vragenlijst (**VK**)
- Onterechte gegevensuitwisseling met GGD GHOR (**OG**)
- Datalek (**DL**)
- Onterechte herleiding (**OH**)

Processtappen

1. Gebruiksgegevens in Formdesk omgeving vóór invullen vragenlijst

1. Verstrekken van heldere informatie over de CONTEST studie via een privacyverklaring (zie **bijlage 9**) en toestemmingsformulier **(VC)**;
2. Duidelijke uitwerking van de beperking van rechten van betrokkenen **(VC)**;
3. Duidelijk benoemen dat de bewaartermijn van de geanonimiseerde dataset permanent is **(VC)**;
4. Om er zeker van te zijn dat enkel volwassenen uit de juiste onderzoekspopulatie deelnemen aan de studie, zijn er diverse checks ingebouwd **(VC)**:
    a. Allereerst staat in de tekst in de e-mail dat enkel volwassenen deel kunnen nemen aan de studie. Vervolgens staat dit opnieuw vermeld bij de omschrijving van de studie in Formdesk;
    b. Daarna moeten de deelnemers aangeven dat ze 18 jaar of ouder zijn, anders krijgen ze een scherm te zien dat ze niet deel mogen nemen aan de studie;
    c. Als laatste moeten de deelnemers hun geboortejaar invullen. Als het ingevulde geboortejaar groter is dan 2002, krijgen ze een foutmelding te zien. Door middel van deze diverse checks zorgen we ervoor dat enkel volwassenen mee doen aan de studie;

goedgekeurde gedragscodes en certificeringsmechanismen.
Ter illustratie noemt de AVG de volgende maatregelen:

a. pseudonimiseren en versleutelen van persoonsgegevens;
b. 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. gebruikscontrole
e. controle op de toegang tot gegevens;
f. transmissiecontrole;
g. invoercontrole;
h. transportcontrole; en
i. herstelmogelijkheid.

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 gegevens 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.

5. Om er zeker van te zijn dat volwassenen die niet in een zorginstelling wonen en/of volwassenen die nog niet hun Covid-19 testuitslag hebben ontvangen deelnemen aan de studie, zijn er diverse checks ingebouwd **(VC)**:
    a. Staat in de tekst in de e-mail dat enkel volwassenen die niet in een zorginstelling wonen en/of volwassenen die nog niet hun Covid-19 testuitslag hebben ontvangen deel kunnen nemen aan de studie. Vervolgens staat dit opnieuw vermeld bij de omschrijving van de studie in Formdesk;
    b. Daarna moeten de deelnemers aangeven dat ze niet in een zorginstelling wonen en dat ze nog niet hun testuitslag hebben ontvangen, anders krijgen ze een scherm te zien dat ze niet deel mogen nemen aan de studie;

2. Invullen vragenlijst in Formdesk

6. Formdesk is alleen beschikbaar via Campus Pro werkplek (beveiligde RIVM-netwerk) op basis van inlognaam en wachtwoord (alleen beschikbaar voor medewerkers) **(DL)**;
7. Dagelijks van maandag tot en met vrijdag worden de ingevulde vragenlijsten uit

Formdesk geëxporteerd. De vragenlijsten worden opgeslagen in een map op de netwerkschijf van het RIVM, waar alleen de direct betrokken onderzoekers toegang toe hebben **(DL)**;

8. Na export worden de ingevulde vragenlijsten uit Formdesk verwijderd. Formdesk zorgt voor een back-up van de aanwezige gegevens. Dit proces verloopt automatisch. De gegevens worden maximaal **1 maand** bewaard. Daarna worden ze automatisch gewist **(DL)**;
9. Dataminimalisatie in de gehele keten als uitgangspunt, zoals gebruik te maken van het geboortejaar i.p.v. geboortedatum en 4-cijferige postcode i.p.v. de volledige postcode **(OH), (DL)**.

3. Verstrekken CoronIT nummers aan GGD GHOR voor labuitslagen (en ontvangen gegevens vanuit GGD GHOR)

10. Deelnemer vult twee keer zijn/haar CoronIT-nummer in zodat koppeling met de juiste informatie vanuit GGD GHOR plaatsvindt **(VC), (OG)**;
11. Pseudonimiseren persoonsgegevens aan de bron (GGD GHOR) **(OG)**;
12. Aanvullende controle door GGD GHOR van gebruik juiste CoronIT-nummer door te checken op overeenstemming van test uitslag, geboortejaar, 4-cijferige postcode tussen ontvangen laboratorium gegevens met ingevulde vragenlijst **(VC), (VK), (OG)**;
13. Verwijdering van de gegevens bij de controle zoals beschreven bij 3.12 indien gegevens niet overeen blijken te komen **(VK)**;
14. De uitwisseling van gegevens tussen GGD GHOR en het RIVM vindt plaats via een beveiligde verbinding (Zorgmail). Dit is een dienst waarmee geauthentiseerde gebruikers veilig en gemakkelijk grote bestanden naar andere gebruikers kunnen verzenden. De e-mails zijn standaard versleuteld **(DL)**;
15. De kwetsbaarheid (URL tampering) die ten grondslag lag aan het incident met Infectieradar kan niet meer voorkomen: er wordt nu gebruik gemaakt van unieke keys met een random waarde in de link naar de vragenlijst. De volgnummers zijn niet meer te raden **(DL)**;
16. Vastleggen van overeenkomsten zoals de DSA tussen het RIVM en GGD GHOR **(OG)**.

4. Samenvoegen labuitslagen en vragenlijsten

17. De laboratoriumuitslagen worden opgeslagen in een map op de netwerkschijf van het RIVM die alleen toegankelijk is voor de direct betrokken onderzoekers **(DL)**;
18. Na controle van de gegevens wordt het CoronIT-nummer vervangen door een studienummer; gebruik maken van een studienummer i.p.v. gebruik te maken van de CoronIT nummers in het analysebestand **(OH)**;
19. Het bestand met de CoronIT-nummers worden na de koppeling direct en definitief verwijderd.
20. Voorafgaand aan de verwijdering van het bestand met CoronIT-nummers zal dit document encrypted zijn door gebruik te maken van 7zip. Dit is een standaard programma dat aangeboden is op de computers van het RIVM. Voor het betreffende document kan een zip file worden aangemaakt met daarop een wachtwoord, waarmee de inhoud encrypt wordt. Daarnaast staat het document opgeslagen in een map op de netwerkschijf van het RIVM die alleen toegankelijk is voor de betrokken onderzoekers en is beveiligd door middel van een wachtwoord **(DL), (OH)**;
21. Het wachtwoord om het tijdelijke (voordat het bestand met CoronIT nummers verwijderd is) sleutelbestand te openen staat vermeld in een ander document die opgeslagen is in een andere map op de netwerkschijf van het RIVM die alleen toegankelijk is voor de betrokken onderzoekers. Benoeming van de betrokken onderzoekers is vastgelegd in het ('levende') protocol **(DL), (OH)**.

5. Analyses

22. Beschikbaarheid van onderzoeksgegevens beperkt tot de rechtstreeks betrokken onderzoekers van het RIVM (<10 onderzoekers)**(DL);**
23. Onderzoeksresultaten die gepubliceerd worden, zijn samengesteld op basis van de analyse van de gegevens. De publicatie vindt plaats zonder herleidbare persoonsgegevens **(VC)**.

6. Archivering

24. Bewaartermijn van het document met de e-mailadressen van de deelnemers is 5 jaar **(VC);**
25. De gegevens in de databases worden zonder herleidbare persoonsgegevens gearchiveerd (geanonimiseerd) **(VC);**
26. In overeenstemming met de rijksbrede hotspot is besloten dat voor de geanonimiseerde dataset een permanent bewaartermijn geld (**VC**).

Algemene maatregelen

27. Het basisbeveiligingsniveau (BBN) van de CONTEST studie is in kaart gebracht door middel van de Quickscan Information Security (QIS), kortweg Quickscan BIO (**Bijlage 6**) **(VC), (OG), (DL);**
28. Toegang tot databestanden alleen voor de direct betrokken onderzoekers: toegang beveiligd door middel van wachtwoorden **(DL), (OH)**;
29. Computer op lock zetten bij afwezigheid **(DL);**
30. Deze PIA wordt ook voorgelegd ter goedkeuring aan de betrokken jurist van GGD GHOR 5.1.2e **(OG);**
31. 2 factor-authentificatie in geval van inloggen in Campus buiten het RIVM **(DL).**
32. Logging op acties in datasets **(DL)**
33. Regelmatige controle op wie toegang heeft tot de onderzoeksdata **(DL);**
34. Monitoring van het RIVM netwerk door afdeling informatiebeveiliging om zo verdacht verkeer te kunnen ontdekken zoals een hack, virus, of malware **(VC);**
35. Back-ups van bestanden opgeslagen op de RIVM netwerkschijf voor een restore bij onrechtmatige vernietiging (**VC**);
36. Het RIVM dient inbreuken in verband met Persoonsgegevens of een vermoeden daarvan onmiddellijk, maar in ieder geval binnen 24 uur bij GGD GHOR te melden zodra er kennis van is genomen (**zie Bijlage 7**) (**DL**).
37. GGD GHOR dient inbreuken in verband met Persoonsgegevens of een vermoeden daarvan onmiddellijk, maar in ieder geval binnen 24 uur na ontdekking aan RIVM te melden op 5.1.2e @rivm.nl (**zie Bijlage 7**) (**DL**).

Bijlagen

Bijlage 1: Protocol

Bijlage 2: Voorbeeld bevestigingsemail

Bijlage 3: Informatie over de studie voor de deelnemers

Bijlage 4: Vragenlijst

Bijlage 5: Analyse informatiebeveiliging

Bijlage 6: Quickscan BIO

Bijlage 7: Data Sharing Agreement

Bijlage 8: E-mail waarin CISO advies IB bevestigd

Bijlage 9: Privacyverklaring