Gegevensbeschermingseffectbeoordeling (PIA)

VWS, RIVM, CIb, EPI, RVP

CONTEST studie naar COVID-19 risicofactoren

Bilthoven, 2 oktober 2020

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

Vaststelling verwerkersverantwoordelijke: 2 oktober 2020
Naam: (10)(2e), (10)(2e), (10)(2e)) (10)(2e)

Advies functionaris voor gegevensbescherming: Selecteer/typ datum
Naam: Typ naam/functie
Advies Privacy officer RIVM: Selecteer/typ datum
Naam: Typ naam/functie
Advies CIO: Selecteer/typ datum
Naam: Typ naam/functie

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: 0.9

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 COVID-19 op de gezondheid kan hebben.

Het doel van de studie is om inzicht te krijgen in de risicofactoren voor een COVID-19 infectie bij volwassenen die een COVID-19 test hebben gehad in een van de 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 degene die zich laten testen en de testuitslagen worden geregistreerd - genaamd CoronIT - wordt beheerd door GGD GHOR. 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 studie en de vragenlijst van deze 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 worden over de studie (***Bijlage 3***). In de informatie

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
- 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
- **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 COVID-19 (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. Dit betreft de volgende (categorieën) gegevens (zie ook ***Bijlage 4***):

Onderzoeksgegevens

- **Demografische gegevens:**
  - CoronIT nummer (pseudoniem)
  - Geboortejaar (algemeen)
  - Geslacht (algemeen)
  - 4-cijferige postcode (algemeen)
  - Geboorteland (algemeen)
  - Geboorteland ouders (algemeen)
  - Opleiding en beroep (algemeen);
- **Gezondheidsgegevens:**
  - COVID-19 blootstelling gerelateerde gegevens, zoals:
    - gebruik van persoonlijke bescherming middelen,
    - contact met geïnfecteerde personen,
    - bijwonen van activiteiten buitenshuis,
    - gebruik van openbaar vervoer,
    - en reizen.
  - COVID-19 gerelateerde symptomen;
  - Vaccinatiestatus en -datum (influenza en BCG vaccinatie);
  - Zwangerschap;
  - Onderliggende ziektes en chronische aandoeningen.

Daarnaast zullen GGD GHOR bepaalde laboratoria gegevens met betrekking tot de COVID-19 test van de deelnemer delen met het RIVM. Het betreft de volgende gegevens:

Laboratoriumgegevens:

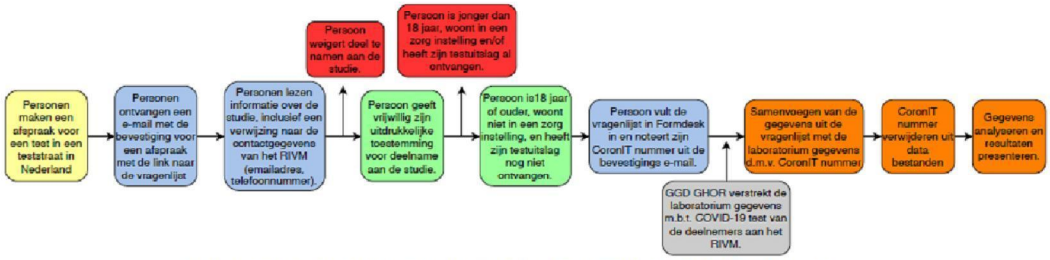
- CoronIT nummer (pseudoniem)
- Laboratorium nummer (pseudoniem)
- Geboortejaar (algemeen)
- 4-cijferige postcode (algemeen)
- Datum test (algemeen)
- Soort afname: keel/ neus (PCR) of bloed (serologie) (bijzonder)

- Teststraat waar de test is afgenomen (algemeen)
- Uitslag test (bijzonder)
- Sequentie van de virusstam (bijzonder)

Waarom persoonsgegevens van de deelnemers worden verzameld staat omschreven in paragraaf 4 'Verwerkingsdoeleinden'.

3. Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer.



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 COVID-19 testuitslag van de deelnemers aan het RIVM via Filesender. De documenten worden opgeslagen op de servers van het RIVM (netwerkschijven). Vervolgens gaan we het unieke CoronIT nummer, waarmee we de gegevens uit de vragenlijst konden samenvoegen met de gegevens uit het laboratorium, vervangen door een studienummer (pseudonimisering). Het CoronIT nummer zal in een ander beveiligd document opgeslagen worden. Dit document zal 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 van de verwerking van de Gegevens staat omschreven in paragraaf 8 'Techniek en methode van gegevensverwerking' en 17 'Maatregelen'.
Voorafgaand aan de studie zal een Data Sharing Agreement (DSA) worden ondertekend door GGD GHOR en het RIVM (***Bijlage 5***). Deze DSA is bedoeld voor de gegevens m.b.t. de laboratorium uitslagen van de deelnemers die GGD GHOR verstrekt aan het RIVM. De GGD'en zullen op de hoogte worden gebracht van het onderzoek maar hebben geen actieve rol in dit onderzoek.

3. Verwerkingsdoeleinden

Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

Klik hier om infotekst te verbergen

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

In Figuur 1 is een schematische weergave van de voorgenomen gegevensverwerking van deze studie te zien. In de figuur is te zien dat deelnemers, na het maken van een test afspraak, een bevestigingsmail van GGD GHOR ontvangen. In deze mail staat een link naar de vragenlijst van de studie. Deelnemers worden uitgenodigd om deel te nemen aan de studie. Deelname aan de studie is op vrijwillige basis. Na het geven van hun toestemming, als ze 18 jaar of ouder zijn en niet in een zorginstelling wonen, kan de vragenlijst worden ingevuld in Formdesk. Formdesk is web-based, ook wel SaaS (Software as a Service) genoemd. SSC Campus beheert namens het RIVM het abonnement van Formdesk, afgesloten met het achterliggende bedrijf Innovero. 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 COVID-19 testuitslag van de deelnemers aan het RIVM via Filesender. De documenten worden opgeslagen op de servers van het RIVM (netwerkschijven). Vervolgens gaan we het unieke CoronIT nummer, waarmee we de gegevens uit de vragenlijst konden samenvoegen met de gegevens uit het laboratorium, vervangen door een studienummer (pseudonimisering). Het CoronIT nummer zal in een ander beveiligd document opgeslagen worden. Dit document zal 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 van de verwerking van de Gegevens staat omschreven in paragraaf 8 'Techniek en methode van gegevensverwerking' en 17 'Maatregelen'.
Voorafgaand aan de studie zal een Data Sharing Agreement (DSA) worden ondertekend door GGD GHOR en het RIVM (***Bijlage 5***). Deze DSA is bedoeld voor de gegevens m.b.t. de laboratorium uitslagen van de deelnemers die GGD GHOR verstrekt aan het RIVM. De GGD'en zullen op de hoogte worden gebracht van het onderzoek maar hebben geen actieve rol in dit onderzoek.

3. Verwerkingsdoeleinden

Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

Klik hier om infotekst te verbergen

De privacyregelgeving geeft als beginsel dat persoonsgegevens enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld. De vaststelling van de verwerkingsdoeleinden is een noodzakelijk voorwaarde om te kunnen beoordelen of de voorgenomen gegevensverwerkingen rechtmatig zijn (onder B) en om vast te stellen welke maatregelen moeten worden getroffen om de risico's (onder C) te voorkomen of verkleinen (onder D). Omschrijf daarom per voorgenomen gegevensverwerking de verwerkingsdoeleinden zo specifiek mogelijk.
Bij verwerkingsdoeleinden kan gedacht worden aan: beveiligen van gebouwen en objecten, behandelen van personeelszaken, opsporen van strafbare feiten, direct marketing, het innen van vorderingen, het doen van leveringen en bestellingen, identificatie en authenticatie, het voorbereiden en nemen van Awb-besluiten en het behandelen van geschillen. Denk ook aan eventuele nevendoeleinden van de gegevensverwerking, zoals: wetenschappelijk, statistisch of historisch onderzoek, archiefbeheer, declaratiedoeleinden, rapportagedoeleinden, verbetering van dienstverlening of (door)ontwikkeling van beleid. De

verwerkingsdoeleinden moeten zoveel mogelijk worden 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.

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.

RIVM
De verwerkersverantwoordelijke is het RIVM, deze stelt namelijk het doel en de middelen vast. De 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 beheert CoronIT, het registratiesysteem van de teststraten. Zij zijn zelfstandig verantwoordelijk voor het verzamelen en verstrekken van de testuitslag gegevens aan het RIVM. GGD GHOR vervult daarmee de rol van verstrekker.

Innovero
Innovero is de leverancier van FormDesk. In FormDesk vullen de deelnemers de vragenlijst in. Innovero verwerkt daarmee in opdracht van het RIVM persoonsgegevens ten behoeve van de CONTEST studie.

SURF (Filesender)
Voor de uitwisseling van persoonsgegevens tussen GGD GHOR en het RIVM wordt gebruik gemaakt van filesender. SURF is hiermee een verwerker van GGD GHOR: zij verwerkt (lees: verstrekt) immers namens GGD GHOR persoonsgegevens van deelnemers aan het RIVM. SURF is hierbij dus GEEN verwerker van het RIVM, maar van de GGD GHOR.

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.

3. 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).

Het algemene belang van dit onderzoek is om meer inzichten te krijgen in de risicofactoren van een COVID-19 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.

3. Verwerkingslocaties

Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

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

3. 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.

Deelnemers vullen eenmalig de vragenlijst in via FormDesk. Dagelijks van maandag tot en met vrijdag zullen de gegevens van de vragenlijsten handmatig uit Formdesk gehaald worden. Dit zal door een van de vijf 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 5 betrokken onderzoekers.

De laboratoriumgegevens van GGD GHOR worden via Filesender beveiligd verzonden naar het RIVM. Ze zullen dit verzenden naar een RIVM e-mailadres die specifiek is aangemaakt voor deze studie. De 5 betrokken onderzoekers 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 netwerkschijf van het RIVM die alleen toegankelijk is voor 2 betrokken onderzoekers. Na deze koppeling wordt een studienummer aangemaakt en worden de CoronIT-nummers uit de databestanden verwijderd en in een ander bestand samen met het studienummer opgeslagen. Zodoende staat in het databestand wat gebruikt wordt voor het analyseren van de data alleen het studienummer en niet het CoronIT nummer. Het 'sleutel' bestand met het CoronIT nummer en het studienummer zal opgeslagen worden op de netwerkschijf van het RIVM in een map die alleen toegankelijk is voor 2 betrokken onderzoekers. Daarnaast zal dit document enkel te openen zijn door middel van een wachtwoord.

Van de deelnemers die hebben aangegeven in de toekomst benaderd te willen worden voor vervolgonderzoek is ook het e-mail adres bij ons bekend. Dit e-mailadres zal na het exporteren van de gegevens uit Formdesk direct worden opgeslagen in een ander bestand. Het bestand met deze e-mail adressen zal worden opgeslagen op de netwerkschijf van het RIVM in een map die alleen toegankelijk is voor 2 betrokken onderzoekers.

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.

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

In het kader van wetenschappelijk onderzoek door het RIVM bepaalt de Archiefwet algemene bewaartermijnen. Het RIVM heeft aan deze algemene bewaartermijnen nadere invulling gegeven. Dit is opgenomen in de Selectielijst RIVM 2004.

Op dit moment is het huidige onderzoek met haar doelstellingen op grond van de Selectielijst RIVM 2004 te classificeren als een *categorie 6* proces. Dit heeft betrekking op het bewaren van gegevens in het kader van wetenschappelijk onderzoek omtrent crises en rampen op het gebied van volksgezondheid, waaronder begrepen het doen van (longitudinaal en retrospectief) wetenschappelijk onderzoek. Voor gegevens die binnen dit proces voor wetenschappelijk onderzoek worden verzameld, geldt vanwege de aard van het proces en de ernst van de situatie een permanente bewaartermijn.

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.

De grondslag(en) voor de verwerking van persoonsgegevens voor deze studie is de uitdrukkelijke toestemming ingevolge artikel 6 lid 1 a AVG.

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. Ingevolge artikel 9 lid 2 sub a AVG is dit verbod is niet van toepassing indien de betrokkene uitdrukkelijk toestemming heeft gegeven. De betrokkene wordt voorafgaand aan de verwerking van diens persoonsgegevens uitdrukkelijke toestemming gevraagd voor de doeleinden zoals omschreven in onderdeel 4. Het verbod op het verwerken van bijzondere persoonsgegevens is dus niet van toepassing op de verzameling van persoonsgegevens voor de CONTEST studie.

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. De verstrekking van die gegevens voor het doeleinde van deze studie is echter rechtmatig, omdat de deelnemer daarvoor zijn toestemming heeft verleend.

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?.

Klik hier om infotekst te verbergen

De privacyregelgeving geeft als beginsel dat de gegevensverwerking wordt beperkt tot wat noodzakelijk is voor de verwerkingsdoeleinden. Dit beginsel van minimale gegevensverwerking/dataminimalisatie komt verder tot uitdrukking door het gebruik van het woord 'noodzakelijk' in artikel 6 AVG en artikel 8 Richtlijn. De AVG en Richtlijn eisen hiermee dat de gegevensverwerking noodzakelijk is voor het verwezenlijken van de doeleinden. De gegevensverwerking moet daarbij voorts de toets aan de beginselen van proportionaliteit en subsidiariteit kunnen doorstaan.

Proportionaliteit betekent dat moet worden beoordeeld of de indringendheid van de voorgenomen gegevensverwerking in een redelijke verhouding staat tot het doel. Bij proportionaliteit wordt gewogen of de realisatie van de verwerkingsdoeleinden zodanig gewicht heeft dat de gegevensverwerkingen, gelet op de mate waarin deze de privacy beperken, deze rechtvaardigen (zijn de beperkingen van het grondrecht en het doel dat met de verwerking wordt beoogd met elkaar in balans?). Daarbij zal onder meer moeten worden gekeken of de voorgenomen gegevensverwerking effectief is om het beoogde doel te bereiken en of de aangevoerde redenen relevant en toereikend zijn om het beoogde doel te bereiken.
Daarbij kunnen empirische onderzoeksresultaten helpen.

Bij subsidiariteit wordt bekeken of de verwerkingsdoeleinden met minder ingrijpende middelen kunnen worden bereikt. Bijvoorbeeld:

- 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.

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, nadat zij hierover conform de voorwaarden in de AVG hierover 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 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. Daarnaast is bij de gegevensverwerking sprake van **subsidiariteit**, omdat: 1. Zonder deze gegevens kunnen de doelstellingen niet bereikt worden; 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. 3. Om te checken of deelnemers het goede CoronIT nummer hebben ingevuld controleren we of het geboortejaar, geslacht en 4-cijferige postcode dat de deelnemer heeft ingevuld in de vragenlijst correspondeert met die gegevens in CoronIT (zodoende moeten we deze gegevens ook van GGD GHOR ontvangen). Op deze manier controleren we 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. 6. Het unieke CoronIT nummer willen we ook na koppeling van de vragenlijst en de testuitslag bewaren om meer gedetailleerde lab data te kunnen koppelen die pas na verder onderzoek door de GGD bekend zijn (zoals sequentie data van de virusstam); 7. 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. Geconcludeerd kan worden dat de overwerkingen 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.

De grondslag van deze studie is op basis van uitdrukkelijke toestemming van de deelnemers. Deelnemers hebben altijd het recht om hun toestemming weer in te trekken. Daarnaast biedt de AVG betrokkenen een aantal rechten, waaronder het recht op inzage, verwijdering of correctie van de gegevens. Gezien (de reden van) de bewaartermijn (permanent) en de pseudonimisatie van de gegevens gelden de volgende beperkingen.

Beperkingen van het recht op inzage, rectificatie of beperking van verwerking

Als de persoonsgegevens worden verwerkt voor wetenschappelijk onderzoek of statistiek, en de nodige voorzieningen (in casu pseudonimisering van de onderzoeksgegevens) zijn getroffen om te verzekeren dat de persoonsgegevens uitsluitend voor statistische of wetenschappelijke doeleinden kunnen worden gebruikt, heeft betrokkene geen recht op inzage, recht op rectificatie en recht op beperking van de verwerking en zal het verzoek worden afgewezen. Dit is overeenkomstig art. 44 van de Uitvoeringswet Algemene Verordening Gegevensbescherming.

Beperkingen van het recht op vergetelheid

In de volgende gevallen heeft betrokkene – overeenkomstig art. 17 AVG – geen recht op vergetelheid en zal het verzoek worden afgewezen:

- Als de persoonsgegevens worden verwerkt voor wetenschappelijk onderzoek of statistische doeleinden en als het recht van betrokkene de verwezenlijking van de doeleinden van de verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen;
- Als de verwerking nodig is om redenen van algemeen belang op het gebied van volksgezondheid;
- Als de verwerking nodig is voor het nakomen van een wettelijke verplichting.

Beperkingen van het recht op bezwaar

Als de verwerking van persoonsgegevens noodzakelijk is voor de uitvoering van een taak van algemeen belang, heeft betrokkene geen recht op bezwaar en zal het verzoek worden afgewezen (art. 21 lid 6 AVG).

Overige beperkingen van de rechten van betrokkenen

Als het RIVM persoonsgegevens verwerkt die door het RIVM niet herleidbaar zijn tot een betrokkene, zijn de rechten van betrokkenen niet van toepassing en zal het verzoek worden afgewezen. Dit is overeenkomstig art. 11 AVG. Concreet betekent dit dat dankzij de pseudonimisering van de onderzoeksgegevens in deze studie ervoor zorgt dat de persoonsgegevens in redelijkheid niet herleidbaar zijn. Het vergt onevenredig veel inspanning om de pseudonimisatie van de gegevens terug te draaien zodat ze weer herleidbaar zijn.

Concluderend betekent dit dat het recht op inzage, rectificatie en vergetelheid in het kader van deze studie beperkt worden op grond van de voorgaande overwegingen en bepalingen.

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.

Klik hier om infotekst te verbergen

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

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

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

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

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

1. Risico's identificeren

De eerste stap is om potentiële privacyrisico's vast te stellen. Een privacyrisico is een kans op het optreden van een negatief gevolg voor de rechten en vrijheden van de betrokkenen als gevolg van de verwerking van

persoonsgegevens.

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

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

2. Risico's inschatten

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

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

De kans dat de risico's zich voltrekken is mede afhankelijk van de middelen die de verwerkingsverantwoordelijke gebruikt bij de gegevensverwerking. Alsook van de aard van de persoonsgegevens.
Persoonsgegevens die de sleutel vormen voor toegang tot geldelijke middelen of waarmee een betrokkene te chanteren is, zijn aantrekkelijk voor hackers. Denk hierbij aan de inloggegevens voor DigiD of een datingwebsite.

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

- vernietiging en verlies (beschikbaarheid);
- wijziging (integriteit);

- ongeoorloofde toegang en verstrekking (vertrouwelijkheid);

van persoonsgegevens, kan leiden tot schade voor de betrokkene.

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

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

3. **Risico's beoordelen**

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

In dit onderdeel worden de potentiële risico's voor betrokkenen beoordeeld. De geconstateerde risico's zijn gecategoriseerd naar type risico vanwege de aard van de risico's. In deze analyse wordt rekening gehouden met de aard, omvang, context en doelstellingen van de gegevensverwerkingen. De risico's worden bepaald door de kans en de impact. Dit bepaalt samen de ernst van het risico. Per risico worden deze twee factoren besproken.

Risico 1: Onrechtmatig gebruik door onbedoelde herleidbaarheid
Hieronder valt het verzamelen van identificeerbare gegevens van deelnemers, het verkeerd koppelen van de ingevulde gegevens uit de vragenlijst met de laboratorium gegevens van de deelnemers en gebruik van de CoronIT-nummers en het includeren van deelnemers jonger dan 18 jaar.

Impact
De negatieve gevolgen bestaan uit het kunnen koppelen van de verwerkte persoonsgegevens aan een geïdentificeerde of identificeerbare natuurlijke persoon door medewerkers of bij een datalek door onbevoegde personen. Zij kunnen dan kennisnemen van de antwoorden in de vragenlijsten. Het feit dat er op die manier bijzondere (medische) persoonsgegevens bekend worden is op zichzelf vanzelfsprekend als ernstig aan te merken, aangezien dit de privacy schendt en tot negatieve gevolgen kan leiden, zoals reputatieschade of uitsluiting. Ook zeer belangrijk is de reputatieschade voor het RIVM, maar ook VWS en de wijdere overheid. Want het vertrouwen van de burger rond haar (data)veiligheid is geschonden. De impact van dit verlies aan vertrouwen rijkt wijder dan alleen dit onderzoek en heeft weerslag in participatie in elk nieuw onderzoek of interactie met de overheid.

Kans
De kans dat er sprake is van onbedoelde herleidbaarheid en onrechtmatig gebruik van de gegevens kan als klein worden beschouwd. Er zijn diverse mitigerende maatregelen getroffen die de kans verkleinen (zie onderdeel D: Maatregelen).

Risico 2: Datalekken
Hieronder valt het onvoldoende beveiligen van de ontvangen en opgeslagen

laboratoriumgegevens, mogelijke toegang van de inlogomgeving van Formdesk door anderen dan de onderzoekers, onvoldoende beveiliging van de e-mailadressen van deelnemers verzameld in het kader van vervolgonderzoek en inzage door deelnemers in andermans gegevens in Formdesk.

Impact:
De impact van datalekken kan zeer hoog zijn, zeker indien daar gevoelige en bijzondere persoonsgegevens bij betrokken zijn. Voor deze studie worden gegevens verwerkt die verband houden met de gezondheid van de deelnemers.

Kans:
De kans op een datalek is klein, omdat de onderzoeksgegevens en het CoronIT-nummer gescheiden opgeslagen worden. Zonder toegang tot beide bestanden is het niet mogelijk deze gegevens aan elkaar te koppelen. Ook zijn de onderzoeksgegevens gepseudonimiseerd, waardoor bij een eventueel datalek de gegevens niet in redelijkheid herleidbaar zijn tot een individuele deelnemer. Daarnaast worden de laboratoriumgegevens via Filesender verstuurd: een beveiligde methode voor verzending van gegevens.

De kans dat er (bijzondere) persoonsgegevens gegevens in het openbaar komen die herleidbaar zijn tot personen is hierdoor zeer gering. Er zijn zes systeembeheerders (2 maal 2-factor authenticatie) die toegang hebben tot de back-end.

Risico 3: Verlies van controle over persoonsgegevens
Hieronder valt de mogelijkheid de gegeven toestemming voor de CONTEST studie weer in te trekken en de (on)bekendheid met gegevens die over deelnemer door GGD GHOR aan het RIVM worden verstrekt. Betrokkenen moeten in principe voorafgaand aan enige verwerking weten wat er met hun persoonsgegevens gebeurt. Hiervoor is het ook van belang dat betrokkenen duidelijk weten welke rechten zij kunnen uitoefenen, en op welke wijze zij dit kunnen doen. Deze rechten zijn niet absoluut, maar dienen wel te allen tijde effectief te zijn.

Impact:
De impact kan hoog zijn omdat betrokkenen vrijwillig persoonsgegevens verstrekken, die bovendien deels van bijzondere aard zijn. Dit veronderstelt dat betrokkenen een hoge mate van vertrouwen hebben in de wijze waarop het RIVM de persoonsgegevens verwerkt. Indien achteraf blijkt dat de gegevens voor andere doeleinden worden gebruikt, of worden verstrekt aan voorheen onbekende partijen dan worden betrokkenen negatief verrast. Dit kan leiden tot reputatieschade voor het RIVM, evenals mogelijke schade voor betrokkenen. Hierbij kan gedacht worden aan materiele en immateriële schade. Dit wordt bevestigd door een uitspraak van de Nederlandse rechtbank waarin is bepaald dat een verlies van controle over persoonsgegevens aangemerkt moet worden als een 'schending van het persoonsrecht' op gegevensbescherming, en dit een grond is betrokkene een schadevergoeding toe te kennen.

Kans:
De kans dat dit risico zich voordoet is laag tot gemiddeld. De studie bevat duidelijke en afgebakende doelstellingen. Vanwege de ontvangst van diverse gegevens vanuit de GGD GHOR is het belangrijk dat hier op een heldere wijze over wordt gecommuniceerd. Verder dient op duidelijke wijze beschreven te worden dat de rechten van betrokkenen zijn beperkt, en waarom dat het geval is.

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.

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

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

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

Voor te treffen maatregelen kan worden aangehaakt bij beveiligingskaders en -standaarden, beste praktijken en goedgekeurde gedragscodes en certificeringsmechanismen.
Ter illustratie noemt de AVG de volgende maatregelen:
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.

Maatregelen: Onrechtmatig gebruik door onbedoelde herleidbaarheid

1. Er worden geen direct herleidbare persoonsgegevens uitgevraagd of verwerkt;
2. 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;
3. Het sleutelbestand met de CoronIT-nummers en studienummers staat opgeslagen in een map op de netwerkschijf van het RIVM die alleen toegankelijk is voor twee betrokken onderzoekers en is beveiligd door middel van een wachtwoord;
4. Het wachtwoord om het sleutelbestand te openen staat vermeld in een ander document die opgeslagen is in een map op de netwerkschijf van het RIVM die alleen toegankelijk is voor twee betrokken onderzoekers;
5. Onderzoeksresultaten die gepubliceerd worden, zijn samengesteld op basis van de analyse van de gegevens. De publicatie vindt plaats zonder herleidbare persoonsgegevens.

Maatregelen: Datalekken

6. Dubbele uitvraag van het CoronIT-nummer aan de deelnemer zodat koppeling met de juiste informatie vanuit GGD GHOR plaatsvindt;

7. Aanvullende controle van gebruik juiste laboratoriumgegevens door ontvangen gegevens (op basis van CoronIT-nummer) vanuit GGD GHOR te checken op overeenstemming van test uitslag, geboortejaar, 4-cijferige postcode met ingevulde vragenlijst;
8. Formdesk is alleen beschikbaar via Campus Pro werkplek (beveiligde RIVM-netwerk) op basis van inlognaam en wachtwoord (alleen beschikbaar voor medewerkers);
9. Beschikbaarheid van onderzoeksgegevens beperkt tot vijf onderzoekers van het RIVM;
10. 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. Na export worden de ingevulde uit Formdesk verwijderd;
11. De laboratoriumuitslagen worden opgeslagen in een map op de netwerkschijf van het RIVM die alleen toegankelijk is voor de direct betrokken onderzoekers;
12. De uitwisseling van gegevens tussen GGD GHOR en het RIVM vindt plaats via een beveiligde verbinding (Filesender). Dit is een webgebaseerde applicatie waarmee geauthenticeerde gebruikers veilig en gemakkelijk willekeurig grote bestanden naar andere gebruikers kunnen verzenden. Verificatie van gebruikers vindt plaats via SimpleSAMLphp, en ondersteunt SAML2, LDAP en RADIUS en meer.

Maatregelen: Verlies controle over persoonsgegevens

13. Vastleggen van overeenkomsten zoals de DSA tussen het RIVM en GGD GHOR;
14. Verstrekken van heldere informatie over de CONTEST studie via een privacyverklaring en toestemmingsformulier;
15. Duidelijke uitwerking van de beperking van rechten van betrokkenen;
16. Duidelijk benoemen dat de bewaartermijn permanent is.

Algemene maatregelen

17. 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.
18. Om er zeker van te zijn dat enkel volwassenen uit de juiste onderzoekspopulatie deelnemen aan de studie, zijn er diverse checks ingebouwd:
    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;
19. 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:
    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;
20. Toegang tot databestanden alleen voor de 5 betrokken onderzoekers: toegang beveiligd door middel van wachtwoorden;
21. Computer op lock zetten bij afwezigheid;

22. Deze PIA wordt ook voorgelegd voor goedkeuring aan GGD GHOR;

Met deze maatregelen zijn zowel specifieke als algemene risico's afgedekt. Tijdens het onderzoek zullen de risico's en maatregelen geëvalueerd worden, zodat op basis van wijzigende omstandigheden of voortschrijdend inzicht de risico's en maatregelen up-to-date blijven.

Bijlagen