



Gegevensbeschermingseffectbeoordeling (PIA)

VWS, RIVM, CIB, EPI, RES

Q-koorts en COVID-19 (deelonderzoek 2, Q-HORT en COVID-19)

Bilthoven, 12 november 2020



VWS, RIVM, CIB, EPI, RES - Q-koorts en COVID-19 (deelonderzoek 2, Q-HORT en COVID-19)

Vaststelling verwerkersverantwoordelijke: 15 oktober 2020

Naam: 5.1.2e 5.1.2e, 5.1.2e 1.2 5.1.2e, 5.1.2e 5.1.2e 5.1.2e, 5.1.2e 5.1.2e 5.1.2e

Advies functionaris voor gegevensbescherming: Selecteer/typ datum

Naam: Typ naam/functie

Advies CIO: 28 oktober 2020

Naam: 5.1.2e 5.1.2e, 5.1.2e 5.1.2e

VWS, RIVM, CIB, EPI, RES - Q-koorts en COVID-19 (deelonderzoek 2, Q-HORT en COVID-19)

Gegevensbeschermingseffectbeoordeling (PIA)

VWS, RIVM, CIB, EPI, RES

Q-koorts en COVID-19 (deelonderzoek 2, Q-HORT en COVID-19)

Contact:

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

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

Versie: 1.0

Inhoudsopgave

A. Beschrijving kenmerken gegevensverwerkingen.....	5
1. Voorstel	5
2. Persoonsgegevens	6
3. Gegevensverwerkingen	9
4. Verwerkingsdoeleinden	10
5. Betrokken partijen	11
6. Belangen bij de gegevensverwerking	12
7. Verwerkingslocaties	13
8. Techniek en methode van gegevensverwerking	13
9. Juridisch en beleidsmatig kader	13
10. Bewaartermijnen	14
B. Beoordeling rechtmatigheid gegevensverwerkingen.....	15
11. Rechtsgrond	15
12. Bijzondere persoonsgegevens	15
13. Doelbinding	16
14. Noodzaak en evenredigheid	16
15. Rechten van de betrokkene	17
C. Beschrijving en beoordeling risico's voor de betrokkenen.....	18
16. Risico's	18
D. Beschrijving voorgenomen maatregelen.....	21
17. Maatregelen	21

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.

Deze gegevensbeschermingseffectbeoordeling (PIA) is bedoeld voor het onderzoek genaamd 'Hebben mensen na het doormaken van Q-koorts een verhoogd risico op infectie met SARS-CoV-2 en op ernstig beloop van COVID-19?', dat wordt uitgevoerd door het Centrum Epidemiologie en Surveillance van Infectieziekten (EPI) van het RIVM. Het doel is om te onderzoeken of, en zo ja, welke relatie er is tussen doorgemaakte Q-koorts en extra kwetsbaarheid voor COVID-19. Om bovenstaande vraag te beantwoorden worden twee oriënterende analyses uitgevoerd en drie deelonderzoeken. Deze PIA heeft betrekking op deelonderzoek 2, genaamd 'Q-HORT en COVID-19'.

Enkele regio's in het oosten van de provincie Noord-Brabant zijn begin 2020 zwaar getroffen door de COVID-19 epidemie. Opvallend is dat dit dezelfde regio's zijn waar tijdens de Q-koorts epidemie van 2007-2010 veel Q-koorts voorkwam. Met het 'Q-koorts en COVID-19' onderzoek wordt bekeken of er een mogelijk verband is met het krijgen van COVID-19 en/of de ernst ervan bij personen die Q-koorts gehad hebben.

Aanleiding voor het onderzoek naar Q-koorts en COVID-19 is een toezegging door minister H.M. de Jonge aan het lid Heerma tijdens het debat van 7 mei 2020 over COVID-19. Op 28 augustus 2020 is de definitieve versie van het onderzoeksvoorstel, genaamd 'Hebben mensen na het doormaken van Q-koorts een verhoogd risico op infectie met SARS-CoV-2 en op ernstig beloop van COVID-19?' ingediend bij VWS (*Bijlage A*). In de 'Kamerbrief stand van zaken COVID-19' van 21 september 2020 (Kamerstuk 25 295, nr 534) heeft minister H.M. de Jonge beschreven dat dit onderzoek in gang is gezet en dat de resultaten voor het eind van het jaar verwacht worden (*Bijlage B*). Op 24 september is de officiële opdrachtbrief ontvangen door het Centrum Infectieziektebestrijding (CIb) van het RIVM (161-2020) (*Bijlage C*).

Voor dit onderzoek worden mensen benaderd die tussen 2011 en 2013 aan onderzoek naar Q-koorts hebben deelgenomen, het Q-HORT onderzoek. Het Jeroen Bosch Ziekenhuis en het RIVM waren de gezamenlijk de coördinatoren/projectleiders van dit onderzoek vanuit een gezamenlijke ZonMw subsidieaanvraag (in huidige termen waren het RIVM en het JBZ beiden verwerkingsverantwoordelijke). 5.1.2e 5.1.2e was de hoofdonderzoeker van het Q-HORT onderzoek. De ruim 1400 deelnemers die toentertijd hebben aangegeven bereid te zijn aan vervolgonderzoek deel te nemen, worden in het kader van deze studie benaderd. De vraag werd als volgt gesteld op de papieren toestemmingsverklaring die de deelnemer destijds invulde: "In de toekomst wordt er mogelijk nog meer wetenschappelijk onderzoek gedaan naar gevolgen van Q-

koorts op de lange termijn. Gaat u ermee akkoord dat u in de toekomst nogmaals benaderd wordt voor onderzoeksdoeleinden?" Vervolgens moesten één van de twee opties actief aangekruist worden: "Ja, ik mag in de toekomst opnieuw benaderd worden" of "Nee, ik wil niet meer benaderd worden voor wetenschappelijk onderzoek". Personen die toestemming gaven worden benaderd na een check van de adresgegevens en het in leven zijn in het Basisregister Persoonsgegevens (zie voor meer details onderdeel C (16) en D (17) van deze PIA). Wanneer dit niet gedaan zou worden dan is het vermoeden dat een aantal nabestaanden of verkeerde personen de uitnodiging ontvangen (na verhuizing/emigratie) en dit is uitermate onwenselijk. We vermoeden 1000-1200 personen die in het verleden Q-koorts doorgemaakt hebben uiteindelijk uit te kunnen nodigen (die dus nog in leven zijn en waarvan een actueel adres beschikbaar is). Personen die willen deelnemen, vullen na uitnodiging tot deelname (zie **Bijlage D**) eenmalig digitaal via Formdesk of op papier een deelname- en toestemmingsformulier (vanaf hier 'deelnameformulier' genoemd) (zie **Bijlage E**) en vragenlijst in (zie **Bijlage F**). In de vragenlijst wordt naast leeftijd en geslacht gevraagd naar de algemene en COVID-19-gerelateerde gezondheid (onderliggende ziekten en of zij in 2020 (en/of 2021, afhankelijk van wanneer de vragenlijst verstuurd gaat worden – dit wordt zo nodig nog aangepast in de vragenlijst en deelnemersinformatie) gezondheidsklachten hebben gehad die te maken kunnen hebben met COVID-19, of zij daarvoor hun huisarts en/of spoedeisende hulp bezocht hebben en/of in het ziekenhuis (al dan niet op de IC) zijn opgenomen en of zij of eventuele huisgenoten positief getest zijn op SARS-CoV-2).

De informatie uit de vragenlijst van deelnemers met doorgemaakte Q-koorts zal vergeleken worden met informatie uit een controlegroep, bestaande uit de reeds bij het RIVM aanwezige gepseudonimiseerde gegevens in OSIRIS van een selectie van personen die gemeld zijn door de GGD-en met een SARS-CoV-2 positieve testuitslag (OSIRIS AIZ meldingen voor COVID-19, zie voor meer details de PIA voor OSIRIS in **Bijlage G**). Slechts een minimale selectie van de beschikbare informatie die beschikbaar is in OSIRIS van deze meldingen zal gebruikt worden om het voorkomen en de ernst van COVID-19 te vergelijken met de deelnemers van de vragenlijst die Q-koorts doorgemaakt hebben. De gegevens in de vragenlijst voor de personen met doorgemaakte Q-koorts zijn afgestemd op de gegevens die in OSIRIS verzameld worden voor COVID-19. Op basis van deze vergelijking wordt onderzocht of Q-koorts mogelijk tot een ernstiger beloop leidt van COVID-19 (bijvoorbeeld vaker sprake van een ziekenhuis- of IC-opname). Tevens zal via een geaggregeerde analyse worden bekeken of personen die Q-koorts doorgemaakt hebben relatief vaker COVID-19 hebben gehad (COVID-19 incidentie) dan in enkele controle gemeentes. De deelnemer kan aangeven om de algemene onderzoeksresultaten te ontvangen per email. Hoewel ook sociale en psychische aspecten een belangrijke rol kunnen spelen bij Q-koorts en COVID-19, is dit onderzoek specifiek opgezet om eventuele medische gevolgen in beeld te brengen.

Deze PIA omschrijft de aspecten rondom de gegevensverzameling en-bescherming van deze studie, en waarborging van de privacy de deelnemers aan deze studie.

In het document wordt over de 'direct betrokken onderzoekers' of het 'projectteam' gesproken. Op dit moment zijn dat 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e en 5.1.2e. Wanneer noodzakelijk voor de uitvoering van het onderzoek zal het projectteam uitgebreid worden.

2. Persoonsgegevens



Som alle categorieën van persoonsgegevens op die worden verwerkt. Geef per categorie van persoonsgegevens tevens aan op wie die betrekking hebben. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder, strafrechtelijk en wettelijk identificerend.

Klik hier om infotekst te verbergen

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

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

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

Gepseudonimiseerde (ook wel: versleutelde) gegevens worden als persoonsgegevens beschouwd. Onder pseudonisering 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, hartaanval, handicap, ziekterisico of verleende gezondheidsdiensten.

Strafrechtelijke persoonsgegevens

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

Wettelijke identificatienummers

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

Overige persoonsgegevens

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

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

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

Betrokkenen

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

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

Bij 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.

Hieronder is per datastap beschreven welke persoonsgegevens verwerkt worden. Data-minimalisatie is op alle stappen toegepast.

1.Q-koorts en COVID-19 dataverzameling

2.

2.1. Adressenbestand Q-HORT onderzoek 2011-2013 - contactgegevens

2.1.1. Data (verouderde adresgegevens):

2.1.2. Algemeen

- Geslacht (algemeen) – nodig voor controle BRP (zie 1.1.2)
- Geboortedatum (algemeen) – nodig voor controle BRP (zie 1.1.2)

- 4-cijferig deelnemersnummer (algemeen) – nodig als unieke identifier in het onderzoek
- - **Contactgegevens**
 - Aanhef, voorletters, naam (algemeen) – nodig voor controle BRP (zie 1.1.2)
 - Adresgegevens - adres, postcode, woonplaats (algemeen) – nodig voor de praktische uitvoer van de actualisatie van adresgegevens
- - 2.1.3. **Data (bestand dat wordt geüpload naar T&T (vertrouwdsverbonden.nl) voor actualisatie adresgegevens) – eerste upload:**
 - 2.1.4. **2.1.5. Algemeen**
 - Geslacht (algemeen) – nodig voor opvragen gegevens uit BRP
 - Geboortedatum (algemeen) – nodig voor opvragen gegevens uit BRP
 - - **Contactgegevens**
 - Achternaam (algemeen) – nodig voor opvragen gegevens uit BRP
 - - 2.1.6. **Data (bestand dat wordt geüpload naar T&T (vertrouwdsverbonden.nl) voor actualisatie adresgegevens) – tweede upload:**
 - 2.1.7. **2.1.8. Algemeen**
 - A-nummer (anoniem BSN nummer, administratief nummer van de persoon bedoeld in de Wet BRP dat is afgeleid van de BSN en is een vast nummer) – nodig om de meest recente adresgegevens op te halen uit het BRP net voor verzending van de vragenlijst
 - - 2.1.9. **Data (geactualiseerde adresgegevens):**
 - 2.1.10. **Algemeen**
 - Geslacht (algemeen) – nodig voor het versturen van de vragenlijst/bepalen aanhef en ter controle van verkeerd ingevulde deelnemersnummers in de digitale vragenlijst
 - Geboortedatum (algemeen) – nodig ter controle van verkeerd ingevulde deelnemersnummers in de digitale vragenlijst (om te vergelijken met de ingevulde leeftijd)
 - Overlijdensdatum – indien van toepassing (algemeen) – nodig om te bepalen wie er in 2020/2021 overleden is (zie 1.4)
 - 4-cijferig deelnemersnummer (algemeen) – nodig als unieke identifier in het onderzoek
 - A-nummer (anoniem BSN nummer, administratief nummer van de persoon bedoeld in de Wet BRP dat is afgeleid van de BSN en is een vast nummer) – nodig voor eventueel vervolgonderzoek om eenvoudig de meest recente adresgegevens opnieuw op te kunnen vragen in het BRP
 - - **Contactgegevens**
 - Aanhef, voorletters, naam (algemeen) – nodig voor het versturen van de vragenlijst
 - Adresgegevens - adres, postcode, woonplaats, gemeente (algemeen) – nodig voor het versturen van de vragenlijst
 - - 2.2. **Vragenlijst Q-koorts en COVID-19 (op papier of digitaal in Formdesk in te vullen door deelnemer) – onderzoeksgegevens**
 - 2.3. **Algemeen**

- 4-cijferig deelnemersnummer (algemeen) – nodig als unieke identifier in het onderzoek
- Datum van invullen (algemeen) – nodig om te bepalen wanneer het formulier ingevuld is en om de bewaartermijn te bepalen
- Geslacht (algemeen) – nodig om controlegroep te kunnen matchen
- Leeftijd in jaren (algemeen) – nodig om controlegroep te kunnen matchen
- Eventuele opmerkingen/aanvullingen op de vragenlijst (algemeen)

• **Gezondheidsgegevens**

- Onderliggende ziektes en chronische aandoeningen (bijzonder) – bekende risicofactor voor COVID-19 en ernstiger beloop, nodig om in de analyses voor te kunnen corrigeren en te vergelijken
- Overgewicht of obesitas (bijzonder) – bekende risicofactor voor COVID-19 en ernstiger beloop, nodig om in de analyses voor te kunnen corrigeren en te vergelijken
- Zwangerschap in 2020 (en/of 2021 afhankelijk van verzending vragenlijst) (bijzonder) – dit is ook onderdeel van de OSIRIS-vragenlijst voor de controlegroep, nodig om te vergelijken
- Doorgemaakte Q-koorts (bijzonder) – als onderscheid tussen de deelnemers met Q-koorts en de controlegroep

• **COVID-19-gerelateerd**

- COVID-19 gerelateerde symptomen in 2020 (en/of 2021 afhankelijk van verzending vragenlijst) (bijzonder) – nodig om deelnemers tot (mogelijk/vermoedelijk) COVID-19 te classificeren (casus definitie) omdat voor 1 juni 2020 een strict testbeleid werd toegepast in Nederland
- Aantal keren COVID-19 gerelateerde symptomen in 2020 (en/of 2021 afhankelijk van verzending vragenlijst) met een periode van minimaal twee weken tussen de klachtenperiodes (1,2,3 of meer dan 3 keer) (bijzonder) – nodig om deelnemers tot (mogelijk/vermoedelijk) COVID-19 te classificeren (casus definitie) omdat voor 1 juni 2020 een strict testbeleid werd toegepast in Nederland
- Eerste ziekte dag (datum) (bijzonder) – nodig om te bepalen wanneer iemand ziek is geweest en te matchen met de controlegroep
- COVID-19 test gedaan (ja/nee, datum en uitslag) (bijzonder) – nodig om personen met vastgestelde COVID-19 te identificeren
- Personen in het huishouden of de thuissituatie die positief getest zijn voor SARS-CoV-2 wanneer bij de persoon zelf geen test is uitgevoerd (bijzonder) – nodig om deelnemers tot (mogelijk/vermoedelijk) COVID-19 te classificeren (casus definitie) omdat voor 1 juni 2020 een strict testbeleid werd toegepast in Nederland
- Medische zorg gehad (ja/nee en door wie: huisarts(enpost), spoedeisende hulp, ziekenopname of intensive care-opname) (bijzonder) – nodig voor het classificeren van de ernst van COVID-19 en dit te vergelijken met de controlegroep

• **2.4. Deelnameformulier Q-koorts en COVID-19 (op papier of digitaal in Formdesk in te vullen door deelnemer) - contactgegevens**

2.5. Algemeen

- 4-cijferig deelnemersnummer (algemeen) – nodig als unieke identifier in het onderzoek

- Datum van invullen (algemeen) – nodig om te bepalen wanneer het formulier ingevuld is en om de bewaartermijn te bepalen
- - **Contactgegevens**
 - Voorletters, naam (algemeen) – nodig om te weten wie het deelnameformulier ingevuld heeft
 - Telefoonnummer (optioneel in te vullen door deelnemer) (algemeen) – nodig voor eventueel vervolgonderzoek of om contact op te nemen met de deelnemers wanneer het deelnameformulier niet volledig is ingevuld
 - Email (optioneel in te vullen door deelnemer) (algemeen) – nodig voor het verzenden van de algemene onderzoeksresultaten of om contact op te nemen met de deelnemers wanneer het deelnameformulier niet volledig is ingevuld en voor eventueel vervolgonderzoek
 - Handtekening (of vinkje bij digitaal toestemming geven) (algemeen) – nodig om vast te stellen dat de deelnemer instemt met deelname
 -
 - **Toestemming**
 - Toestemming om ingevulde (adres)gegevens op te slaan voor eventueel vervolgonderzoek (algemeen)
 - Wel/niet per email op de hoogte gesteld willen worden over de algemene onderzoeksresultaten (algemeen)
-
- 2.6. **Deelnemers aan Q-HORT studie die in 2020-2021 zijn overleden (bestand dat naar de GGD Hart voor Brabant wordt gestuurd) - contactgegevens**
- 2.7. **Algemeen**
 - 4-cijferig deelnemersnummer (algemeen) – nodig als unieke identifier in het onderzoek
 - Geslacht (algemeen) – nodig voor het opzoeken van de persoon in HPZone (het elektronisch patiëntendossier van de GGD)
 - Geboortedatum (algemeen) – nodig voor het opzoeken van de persoon in HPZone
-
- **Contactgegevens**
 - Aanhef, voorletters, naam (algemeen) -- nodig voor het opzoeken van de persoon in HPZone
-
- 2.8. **Deelnemers aan Q-HORT studie die in 2020-2021 zijn overleden en die bij de GGD geregistreerd staan als COVID-19 positief (bestand dat van de GGD Hart voor Brabant naar het RIVM wordt gestuurd) – onderzoeksgegevens**
- 2.9. **Algemeen**
 - 4-cijferig deelnemersnummer (algemeen) – nodig als unieke identifier in het onderzoek
-
- **Gezondheidsgegevens**
 - OSIRIS nummer van COVID-19 melding (algemeen) – nodig om de benodigde gegevens uit de OSIRIS melding te halen (zie 2.2)
-
- 2.10. **Adresbestand personen die toestemming geven voor eventueel vervolgonderzoek naar Q-koorts en COVID-19 - contactgegevens**
- 2.11. **Algemeen**
 - 4-cijferig deelnemersnummer (algemeen) – nodig als unieke identifier in het onderzoek

- Geslacht (algemeen) – nodig voor het bepalen van de aanhef
- Geboortedatum (algemeen) – nodig voor het uitnodigen voor eventueel vervolgonderzoek van een specifieke leeftijdsgroep binnen personen die Q-koorts doorgemaakt hebben en eventuele toekomstige controle in het BRP
- **Contactgegevens**
 - Aanhef, voorletters, naam (algemeen) – nodig voor het uitnodigen voor eventueel vervolgonderzoek
 - Adresgegevens – adres, postcode, woonplaats, gemeente (algemeen) – nodig voor het uitnodigen voor eventueel vervolgonderzoek
 - Emailadres (optioneel in te vullen door deelnemer) (algemeen) – nodig voor het uitnodigen voor eventueel vervolgonderzoek
 - Telefoonnummer (optioneel in te vullen door deelnemer) (algemeen) – nodig voor eventueel vervolgonderzoek
- **2.12. Koppelbestand voor personen die toestemming geven voor eventueel vervolgonderzoek naar Q-koorts en COVID-19 – contactgegevens**
- **2.13. Algemeen**
 - 4-cijferig deelnemersnummer (algemeen) – nodig als unieke identifier in het onderzoek
 - A-nummer (anoniem BSN nummer, administratief nummer van de persoon bedoeld in de Wet BRP dat is afgeleid van de BSN en is een vast nummer) – nodig voor eventueel vervolgonderzoek om eenvoudig de meest recente adresgegevens opnieuw op te kunnen vragen in het BRP
-
-

3.COVID-19 OSIRIS meldingen

4.

4.1. Controlegroep COVID-19 OSIRIS meldingen – onderzoeksgegevens controlegroep

- 4.2.** Alleen gegevens die vergelijkbaar zijn met de gegevens in de Q-koorts en COVID-19 vragenlijst worden uit de OSIRIS meldingen gehaald zodat een vergelijking mogelijk is. Het is een passieve dataverzameling van gepseudonimiseerde gegevens die al beschikbaar zijn in OSIRIS op basis van het algemeen belang (zie *Bijlage G*). Per deelnemer met een ingevulde vragenlijst zullen COVID-19 OSIRIS meldingen geselecteerd worden om de uitkomsten uit de vragenlijst mee te kunnen vergelijken. COVID-19 meldingen zullen gematcht worden aan deelnemers aan het onderzoek op basis van leeftijd, geslacht, wanneer iemand ziek is geweest en gemeente (controles in Noord-Brabant en controles buiten Noord-Brabant waar wel COVID-19 engszins vergelijkbaar was (delen van Gelderland/Overijssel) maar Q-koorts juist veel lager). Vervolgens worden de volgende gegevens gebruikt voor de analyses:

4.3.

4.4. Algemeen

- Geslacht (algemeen) – nodig om te kunnen matchen aan deelnemer die Q-koorts heeft doorgemaakt
- Leeftijd in jaren (algemeen) – nodig om te kunnen matchen aan deelnemer die Q-koorts heeft doorgemaakt
- Gemeente (algemeen) – nodig om gebieden in Nederland te selecteren (controles in Noord-Brabant en controles buiten Noord-Brabant waar wel COVID-19 engszins vergelijkbaar was (delen van Gelderland/Overijssel) maar Q-koorts juist veel lager)

- Meldende GGD (algemeen) – nodig om te weten wie de eigenaar van de meldingsgegevens is
- Opmerkingen van de GGD aan het RIVM (algemeen) – hier staat aanvullende en mogelijk nuttige informatie in die niet standaard in de melding vermeld kan worden
-
- **Gezondheidsgegevens**
- OSIRIS nummer (algemeen) – unieke identifier van de controle
- Meldingsdatum GGD (algemeen) – nodig voor het bepalen wanneer de melding is gedaan
- Onderliggende chronische aandoeningen (dit is slechts beschikbaar voor een deel van de meldingen vanwege aanpassingen in de OSIRIS vragenlijst) (bijzonder) – bekende risicofactor voor COVID-19 en ernstiger beloop, nodig om in de analyses voor te kunnen corrigeren en te vergelijken met de onderzoeksgroep
- Zwangerschap (dit is slechts beschikbaar voor een deel van de meldingen vanwege aanpassingen in de OSIRIS vragenlijst) (bijzonder) – nodig om in de analyses voor te kunnen corrigeren en te vergelijken met de onderzoeksgroep
- COVID-19 gerelateerde symptomen (bijzonder) (dit is slechts beschikbaar voor een deel van de meldingen vanwege aanpassingen in de OSIRIS vragenlijst) – nodig om te vergelijken met een deelnemer die Q-koorts heeft doorgemaakt
- Eerste ziekte dag (geschat/vastgesteld) en datum eerste ziekte dag (bijzonder) – nodig om te bepalen wanneer iemand klachten had en hierop te matchen met een deelnemer die Q-koorts heeft doorgemaakt
- Datum positieve coronatest (bijzonder) – nodig om te bepalen wanneer iemand klachten had en hierop te matchen met een deelnemer die Q-koorts heeft doorgemaakt
- Medische zorg gehad (ja/nee en door wie: spoedeisende hulp, ziekenopname of intensive care-opname) (bijzonder) – nodig om de ernst te kunnen vergelijken
- Overleden (bijzonder) – nodig om de ernst te kunnen vergelijken
-

4.5. OSIRIS meldingen van deelnemers aan Q-HORT studie die in 2020-2021 zijn overleden en die bij de GGD geregistreerd staan als COVID-19 positief (na check GGD Hart voor Brabant) - onderzoeksgegevens

4.6. Algemeen

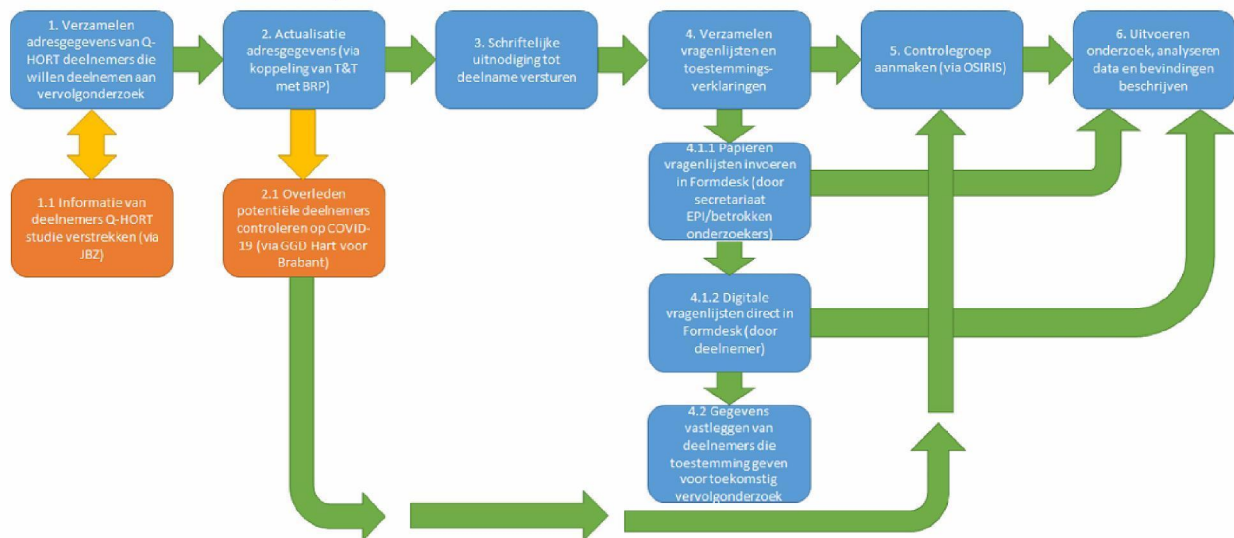
- 4-cijferig deelnemersnummer (algemeen) – nodig als unieke identifier in het onderzoek
- Geslacht (algemeen) – nodig om controlegroep te kunnen matchen
- Leeftijd in jaren (algemeen) – nodig om controlegroep te kunnen matchen
- Gemeente (algemeen) – nodig om gebieden in Nederland te selecteren (controles in Noord-Brabant en controles buiten Noord-Brabant waar wel COVID-19 engszins vergelijkbaar was (delen van Gelderland/Overijssel) maar Q-koorts juist veel lager)
- Meldende GGD (algemeen) – nodig om te weten wie de eigenaar van de meldingsgegevens is
- Opmerkingen van de GGD aan het RIVM (algemeen) – hier staat aanvullende en mogelijk nuttige informatie in die niet standaard in de melding vermeld kan worden
-
- **Gezondheidsgegevens**

- OSIRIS nummer van COVID-19 melding (algemeen) – unieke Identifier van de OSIRIS melding
- Meldingsdatum GGD (algemeen) – nodig voor het bepalen wanneer de melding is gedaan
- Onderliggende chronische aandoeningen (dit is slechts beschikbaar voor een deel van de meldingen vanwege aanpassingen in de OSIRIS vragenlijst) (bijzonder) – bekende risicofactor voor COVID-19 en ernstiger beloop, nodig om in de analyses voor te kunnen corrigeren en te vergelijken
- Zwangerschap (dit is slechts beschikbaar voor een deel van de meldingen vanwege aanpassingen in de OSIRIS vragenlijst) (bijzonder) – dit is ook onderdeel van de OSIRIS-vragenlijst voor de controlegroep, nodig om te vergelijken
- COVID-19 gerelateerde symptomen (bijzonder) (dit is slechts beschikbaar voor een deel van de meldingen vanwege aanpassingen in de OSIRIS vragenlijst) – nodig om deelnemers tot (mogelijk/vermoedelijk) COVID-19 te classificeren (casus definitie) omdat voor 1 juni 2020 een strict testbeleid werd toegepast in Nederland
- Eerste ziektedag (geschat/vastgesteld) en datum eerste ziektedag (bijzonder) – nodig om te bepalen wanneer iemand ziek is geweest en te matchen met de controlegroep
- Datum positieve coronatest (bijzonder) – nodig om te bepalen wanneer iemand klachten had en hierop te matchen de controlegroep
- Medische zorg gehad (ja/nee en door wie: spoedeisende hulp, ziekenopname of intensive care-opname) (bijzonder) – nodig voor het classificeren van de ernst van COVID-19 en dit te vergelijken met de controlegroep
- Overleden (bijzonder) – nodig voor het classificeren van de ernst van COVID-19 en dit te vergelijken met de controlegroep

3. Gegevensverwerkingen



- Geef alle voorgenoemen gegevensverwerkingen weer.



- Deelnemers aan de Q-HORT studie die werd uitgevoerd door het Jeroen Bosch Ziekenhuis (JBZ) en het RIVM, uitgevoerd tussen 2011 – 2013, worden uitgenodigd voor deelname aan deze studie. Hiervoor wordt bij het JBZ de gegevens van deelnemers aan de Q-HORT studie geraadpleegd en op basis van de deelnameformulieren van dat onderzoek bepaald welke deelnemers hebben aangegeven aan vervolgonderzoek te willen deelnemen. De adressen van deze deelnemers worden in een adresbestand samengevoegd. Dit bestand worden beveiligd met een wachtwoord en voorzien van encryptie opgeslagen op de netwerkschijf van het RIVM in de projectmap met beperkte toegang (alleen de direct betrokken onderzoekers, momenteel 4 RIVM-medewerkers, wanneer noodzakelijk voor de uitvoer van dit project dat dit mogelijk nog uitgebreid worden).
- Na samenstelling van het adresbestand met potentiële deelnemers worden de adresgegevens geactualiseerd. Deze actualisatie wordt uitgevoerd door een data-analist van de afdeling Rekenen Data en GIS (RDG) van het RIVM (RDG valt voort bij SSC Campus) middels een webservice van de firma T&T (vertrouwdsverbanden.nl) met behulp van de Basisregistratie Personen (BRP). Er is een verwerkersovereenkomst afgesloten tussen T&T en het RIVM. Het adresbestand van Q-HORT deelnemers wordt beveiligd met een wachtwoord opgestuurd naar een data-analist van de afdeling RDG van het RIVM om de gedateerde adresgegevens te actualiseren en te controleren of personen overleden of geëmigreerd zijn. Het wachtwoord wordt mondeling door **5.1.2e** doorgegeven aan de data-analist. Het bestand wordt voor de duur van dit onderzoek opgeslagen binnen de BRP/GBA-projectmap op de RIVM netwerkschijf (waar in totaal 8 collega's van SSC Campus toegang toe hebben) en wordt naast het wachtwoord ook voorzien van encryptie. De BRP

controle vindt plaats binnen een beveiligde webservice via de firma T&T. Het adresbestand dient geactualiseerd te worden naar het huidige adres en tevens moet gecontroleerd worden of de personen niet inmiddels overleden of geëmigreerd zijn door middel van de BRP voordat de uitnodigingen voor het onderzoek verstuurd kunnen worden (de adressen zijn namelijk 7-9 jaar oud en het is een relatief oude populatie). Dit is noodzakelijk om te voorkomen dat reeds overleden, nabestaanden of geëmigreerde personen de uitnodiging voor dit onderzoek ontvangen. Het geactualiseerde adresbestand wordt beveiligd met een wachtwoord dat alleen bekend is bij het projectteam en voorzien van encryptie opgeslagen op de netwerkschijf van het RIVM in de projectmap met beperkte toegang (alleen de direct betrokken onderzoekers).

• Levende potentiële deelnemers ontvangen een verzoek tot deelname aan dit onderzoek. Deelname aan de studie is vrijwillig. Het schriftelijke verzoek bevat een korte brief met de adresgegevens en uitnodiging tot deelname op RIVM-briefpapier, de deelnemersinformatie (zie **Bijlage D**), twee deelnameformulieren (zie **Bijlage E**), een schriftelijke vragenlijst (zie **Bijlage F**) en een retourenvelop (met de vermelding 'VERTROUWELIJK' erop). In de korte brief en in de deelnemersinformatie wordt de optie geboden het deelnameformulier en de vragenlijst digitaal via Formdesk in te vullen. Hiervoor heeft de deelnemer diens 4-cijferige deelnemersnummer nodig die op het papieren deelnameformulier en de vragenlijst vermeld staan. Deelnemers krijgen drie weken de tijd om deel te nemen. De invoer van het deelnemersnummer is verplicht om verder te kunnen gaan naar het deelnameformulier en de vragenlijst. Ieder nummer kan slechts éénmalig ingevoerd worden en deelnemers kunnen hun ingevulde gegevens dus niet meer terugzien. Indien het deelnameformulier en de vragenlijst op papier worden ingevuld, komt de retourenvelop met "VERTROUWELIJK" erop binnen bij het secretariaat van Centrum EPI. De geretourneerde papieren deelnameformulieren en vragenlijsten zullen voor en na digitalisatie apart van elkaar bewaard worden in een afgesloten kast bij Centrum EPI (sleutel alleen beschikbaar voor het projectteam en het secretariaat van het Centrum EPI). Dit is nodig om de onderzoeksgegevens bij een vermoeden van fouten na digitalisatie te controleren. Digitalisatie van de papieren vragenlijsten gebeurt door het secretariaat van EPI en/of de betrokken onderzoekers via Formdesk. Zij hebben ambtshalve een beroepsgeheim. Het secretariaat heeft geen toegang tot de beveiligde map op de netwerkschijf van het RIVM. Na afronding van de digitalisatie van alle deelnameformulieren en vragenlijsten en het opschonen van het vragenlijstbestand zullen deze apart van elkaar opgeslagen worden in het Centraal Archief van het RIVM.

- De naam en andere direct identificerende gegevens die op het deelnameformulier ingevuld worden, worden apart bewaard van de vragenlijstgegevens op de RIVM-netwerkschijf die alleen voor het projectteam toegankelijk is, beveiligd met een wachtwoord dat ook alleen bij het projectteam bekend is en voorzien van encryptie. Alleen met toegang tot de contactgegevens (bestand deelnameformulier of adresbestand) in combinatie met het deelnemersnummer zijn de vragenlijstgegevens te herleiden. Deze bestanden met contactgegevens en het koppelbestand (deelnemersnummer en A-nummer) blijven bij het projectteam en zijn beveiligd met verschillende wachtwoorden en voorzien van encryptie opgeslagen in de map op de RIVM-netwerkschijf die alleen voor het projectteam toegankelijk is. De ingevulde vragenlijsten worden iedere werkdag uit Formdesk geëxporteerd naar Excel. Na de export worden de ingevulde gegevens in het deelnameformulier (plus het deelnemersnummer) in een apart Excel bestand opgeslagen en de vragenlijstgegevens (plus het deelnemersnummer) in een apart Excel bestand. Beide bestanden worden opgeslagen op de netwerkschijf in de projectmap met beperkte toegang (enkel het projectteam) en vervolgens uit Formdesk verwijderd. De bestanden met de gegevens uit de

deelnameformulieren worden beveiligd met een wachtwoord en voorzien van encryptie. Na afronding van de invoer van alle vragenlijsten zal er van de losse Excel vragenlijstbestanden één bestand gemaakt worden met alle gegevens erin en hetzelfde wordt gedaan voor alle Excel deelnameformulier bestanden. Deze worden op in dezelfde map opgeslagen en op dezelfde manier beveiligd als de losse bestanden. Analyse vindt plaats met behulp van SAS/SPSS/R/STATA en Excel.

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. Op het gebruik van Formdesk is een beveiligingsanalyse uitgevoerd voor dit onderzoek door de CISO-RIVM en daarin is het volgende geconcludeerd (zie voor meer details **Bijlage H en I**). Formdesk is de voorkeursapplicatie binnen het RIVM voor vragenlijstonderzoek. Formdesk is inmiddels in totaal 3 keer onderwerp geweest van een penetratietest (uitgevoerd in opdracht van het RIVM), waarvan 2 zijn uitgevoerd na het bewuste incident. Hieruit zijn geen 'show stoppers' naar voren gekomen. Formdesk laat zelf ook regelmatig pentests uitvoeren op hun dienst. De Formdesk servers zijn onder gebracht in het datacenter van The Datacenter Group in Delft. Dit datacenter is een van de meest geavanceerde datacenters op het gebied van beveiliging, klimaatcontrole en redundantie. Het datacenter is ISO 27001, ISO 9001 en NEN 7510 gecertificeerd. Daarnaast is er na het incident opnieuw een uitgebreide risicoanalyse uitgevoerd, waarbij de conclusie was dat Formdesk als oplossing ingezet kan worden voor het ondersteunen van onderzoeken. De kwetsbaarheid (URL tampering) die ten grondslag lag aan het incident met Infectieradar is hier niet van toepassing, omdat de vragenlijsten maar éénmalig ingevuld kunnen worden.

-
- Deelnemers worden gevraagd of zij bereid zijn in de toekomst deel te nemen aan eventueel vervolgonderzoek op het gebied van Q-koorts en COVID-19. Indien een deelnemer hiervoor toestemming geeft dan geeft hij/zij dit aan op het deelnameformulier. De bij de onderzoekers bekende adresgegevens en eventueel op het deelnameformulier ingevulde emailadres/telefoonnummer worden in een apart adressenbestand voor toekomstig onderzoek opgeslagen (zie 2.1.6) en beveiligd met een wachtwoord dat alleen bekend is bij het projectteam en voorzien van encryptie opgeslagen op de netwerkschijf van het RIVM in de projectmap met beperkte toegang (alleen het projectteam). Dit bestand staat dus helemaal los van de ingevulde vragenlijstgegevens.
-
- Om inzicht te krijgen in de mogelijke ernst van COVID-19 bij personen die Q-koorts doorgemaakt hebben, wordt onderzocht of de overleden potentiële deelnemers in 2020-2021 gemeld zijn bij de GGD met COVID-19. Dit zal uitgevoerd worden door de GGD Hart voor Brabant waarbij zij bij een match het OSIRIS nummer met deelnemersnummer zullen rapporteren aan het projectteam. Op die manier kunnen de betrokken onderzoekers de juiste OSIRIS melding opzoeken en de selectie van gepseudonimiseerde gegevens die van deze personen gerapporteerd zijn in OSIRIS (zie 2.2.2.) worden meegenomen in het onderzoek. (zie 2.2.2.). Het is een passieve dataverzameling van gepseudonimiseerde gegevens die al beschikbaar zijn in OSIRIS op basis van het algemeen belang (zie **Bijlage G**).
-
- Om de onderzoeksgegevens te kunnen vergelijken en om mogelijke verschillen tussen personen met en zonder doorgemaakte Q-koorts met betrekking tot het risico op COVID-19 en de ernst van het beloop te onderzoeken, dient een controlegroep samengesteld te worden. Hiervoor

wordt een selectie gemaakt uit de COVID-19 meldingen in OSIRIS (zie de PIA voor OSIRIS, versie 2, maart 2020 (*Bijlage G*)). Per deelnemer met een ingevulde vragenlijst zullen COVID-19 OSIRIS meldingen geselecteerd worden om de uitkomsten uit de vragenlijst mee te kunnen vergelijken. COVID-19 meldingen zullen gematcht worden aan deelnemers aan het onderzoek op basis van leeftijd, geslacht, wanneer iemand ziek is geweest en gemeente (controles in Noord-Brabant en controles buiten Noord-Brabant waar wel COVID-19 engszins vergelijkbaar was (delen van Gelderland/Overijssel) maar Q-koorts juist veel lager). Deze gegevens in OSIRIS zijn verzameld op basis van het algemeen belang en voor het initiële doel van vroegwaarschuwing, monitoring, surveillance en bestrijding van infectieziekten en daarmee ter bescherming van de volksgezondheid. Vervolgens kan met deze gegevens wetenschappelijk onderzoek worden uitgevoerd (zoals het geval is bij het onderzoek waarop deze PIA van toepassing is) om meer kennis op te doen over incidentie, prevalentie en bestrijding van infectieziekten, o.a. om in de toekomst betere preventiemaatregelen te kunnen nemen. Deze verdere verwerking (in de vorm van wetenschappelijk onderzoek) is verenigbaar met het doel waarvoor de gegevens oorspronkelijk zijn verzameld (art. 5, lid 1(b) AVG en overeenkomstig art 89 lid 1 AVG (zie *Bijlage G*)).

-
- Tot slot worden de gegevens geanalyseerd en resultaten gepresenteerd. Deze (statistische) resultaten bevatten geen (indirect) herleidbare persoonsgegevens, maar zijn slechts op geaggregeerd niveau weergegeven. Op verzoek van VWS zal er een publicatie geschreven worden over de resultaten (hoogstwaarschijnlijk gezamenlijk met de verschillende deelonderzoeken). Mogelijk wordt er ook nog een wetenschappelijk artikel geschreven. Indien het voor publicatie van het artikel nodig is om de onderzoeksgegevens vrij te geven dan zal de dataset met vragenlijstgegevens eerst geanonimiseerd worden zodat deze niet meer herleidbaar is. De algemene geaggregeerde onderzoeksresultaten worden per email aan de deelnemer verstrekt, indien de deelnemer heeft aangegeven dit te willen ontvangen.

4. Verwerkingsdoeleinden



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

[Klik hier om infotekst te verbergen](#)

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

Bij verwerkingsdoeleinden kan gedacht worden aan: beveiligen van gebouwen en objecten, behandelen van personeelszaken, opsporen van strafbare feiten, direct marketing, het innen van vorderingen, het doen van leveringen en bestellingen, identificatie en authenticatie, het voorbereiden en nemen van Awb-besluiten en het behandelen van geschillen. Denk ook aan eventuele nevendoeleinden van de gegevensverwerking, zoals: wetenschappelijk, statistisch of historisch onderzoek, archiefbeheer,

declaratiedoeleinden, rapportagedoeleinden, verbetering van dienstverlening of (door)ontwikkeling van beleid. De verwerkingsdoeleinden moeten zoveel mogelijk worden 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 bedoeld op gebruik van persoonsgegevens die al eerder voor een bepaald doel zijn verzameld. Denk hierbij aan verstrekkingen van persoonsgegevens aan een andere organisatie die niet oorspronkelijk, ten tijde van het verzamelen van de gegevens, was beoogd.

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

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

In dit onderzoek wordt onderzocht of mensen na het doormaken van Q-koorts een verhoogde kans hebben op COVID-19, de ziekte veroorzaakt door het nieuwe coronavirus. Verder wordt onderzocht of COVID-19 ernstiger verloopt bij mensen die Q-koorts hebben gehad. Met ernstiger bedoelen we bijvoorbeeld opname in het ziekenhuis of op de Intensive Care (IC) of overleden ten gevolge van COVID-19. Sociale en psychische aspecten kunnen ook een belangrijke rol spelen bij Q-koorts en COVID-19. Het onderhavige onderzoek is echter slechts opgezet om eventuele medische gevolgen in beeld te brengen.

5. Betrokken partijen



- **Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen:**

verwerkingsverantwoordelijke, verwerker, verstrekker en ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

-
-
- **RIVM**

De verwerkingsverantwoordelijke is het RIVM, deze stelt namelijk het doel en de middelen vast. De rechtstreeks betrokken onderzoekers van het RIVM coördineren de studie, bundelen de gegevens, voeren de analyses uit en hebben toegang tot de gekoppelde gegevens van de deelnemers. Het RIVM is tevens ontvanger van het bestand dat door de GGD Hart voor Brabant wordt samengesteld (zie hieronder).

-
- **Jeroen Bosch Ziekenhuis**
- In het METC protocol van de Q-HORT studie staat dat het onderzoeksteam toegang heeft tot de onderzoeksgegevens. **5.1.2e** **5.1.2e** was lid van dit onderzoeksteam en heeft in die hoedanigheid dus toegang tot deze gegevens. Om gegevens niet overal te hebben staan (veiligheidsoverwegingen) is destijds besloten om deze bij het JBZ op te slaan (zoals beschreven in het METC protocol van de Q-HORT studie). Het RIVM en het JBZ waren feitelijk gezamenlijk verantwoordelijk voor de Q-HORT studie en de daarbij behorende gegevens (in huidige termen verwerkingsverantwoordelijken). Het RIVM verstrekt de gegevens van de Q-HORT studie dus aan zichzelf (via het JBZ).
-
- **Vertrouwdsverbonden.nl (T&T)**
- Het RIVM heeft op grond van het autorisatiebesluit van 30 juli 2014, 2014-0000415392 toegang tot de systematische verstrekking van gegevens uit de basisregistratie personen. T&T biedt via diensten een technische oplossing voor de koppeling met het BRP. In die hoedanigheid verwerkt T&T namens het RIVM gegevens uit het BRP ten behoeve van de taken van het RIVM als bedoeld in artikel 3 Wet op het RIVM. T&T fungeert hiermee als verwerker van het RIVM. Er is een verwerkersovereenkomst tussen het RIVM en T&T.
-
- **GGD Hart voor Brabant**
- Verstrekker. De GGD zal nagaan of personen die in 2020-2021 overleden zijn al dan niet bij hen bekend zijn met een melding voor COVID-19 en zo ja onder welk OSIRIS nummer. Er wordt hiervoor een *Data Sharing Agreement* (DSA) (**Bijlage J**) opgesteld tussen het RIVM en de GGD Hart voor Brabant (de versie in de bijlage is goedgekeurd namens het RIVM en is naar de GGD Hart voor Brabant gestuurd ter controle/ondertekening).
-
- **SURF (FileSender)**

Voor de uitwisseling van persoonsgegevens tussen het JBZ en het RIVM en de GGD Hart voor Brabant en het RIVM wordt gebruik gemaakt van FileSender (**Bijlage H en I**). FileSender is een centraal door het RIVM, via SURF geleverde dienst. Er bestaat een verwerkersovereenkomst tussen het RIVM en SURF voor deze dienst. We maken gebruik van de website filesender.rivm.nl. Na een uitnodiging via email van het RIVM kan het JBZ/de GGD via een weblink een bestand met gegevens van de deelnemers uploaden – deze verbinding verloopt via TLS (1.2). Verdere encryptie (end-to-end) wordt ingesteld door middel van een in te stellen wachtwoord op het downloaden van het bestand. De browser ver- en ontsleutelt bestanden tijdens het up- en downloaden. Dit wachtwoord wordt mondeling doorgegeven aan een van de leden van het projectteam. Door middel van een link

die toegevoegd is aan de email naar JBZ/GGD (geldigheid link maximaal 2 dagen), kan JBZ/GGD via filesender.rivm.nl de databestanden uploaden en doorgeven aan het RIVM. SURF is hiermee een verwerker van het RIVM: zij verwerkt (lees: verstrekt) immers op verzoek van het RIVM persoonsgegevens van deelnemers aan het RIVM.

• **Innovero (Formdesk)**

Innovero is de leverancier van Formdesk. Met Innovero is een verwerkersovereenkomst afgesloten. In Formdesk vullen de deelnemers de digitale vragenlijst in. Papieren vragenlijsten worden na ontvangst door het secretariaat van EPI en/of de betrokken onderzoekers ingevoerd in Formdesk. Innovero verwerkt daarmee in opdracht van het RIVM persoonsgegevens ten behoeve van het onderzoek naar Q-koorts en COVID-19. Formdesk is binnen het RIVM de voorkeursapplicatie voor digitaal vragenlijstonderzoek (voor meer details zie **Bijlage H en I**).

• **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. Alle certificeringen zijn in orde. Equinix is eigenlijk het 'ODC', oftewel Overheids DataCenter.

OSIRIS AIZ

Met behulp van OSIRIS AIZ worden gepseudonimiseerde gegevens van controles geselecteerd die reeds aanwezig zijn bij het RIVM uit OSIRIS AIZ. OSIRIS AIZ is het systeem waarmee de meldingsplichtige infectieziekten in Nederland worden geregistreerd en waarmee het RIVM deze monitort in het kader van de wet publieke gezondheid, met als uiteindelijke doel de lokale en nationale bestrijding van infectieziekten. In OSIRIS AIZ zijn slechts gegevens opgenomen die door de GGD aan de bron zijn gepseudonimiseerd. Het RIVM is dus – zonder medewerking van de GGD – niet in staat deze gegevens te herleiden. De gepseudonimiseerde gegevens uit OSIRIS AIZ worden verwerkt in het kader van de bestrijding van infectieziekten, en in dat kader worden deze gegevens door het RIVM voor dit onderzoek verstrekt (zie **Bijlage G**).

6. Belangen bij de gegevensverwerking



- **Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenomen gegevensverwerkingen.**
-
-
- **Ministerie van Volksgezondheid, Welzijn en Sport**
- Op verzoek van VWS wordt dit onderzoek uitgevoerd. Het algemene belang is om meer inzicht te krijgen in de mogelijke relatie tussen doorgemaakte Q-koorts en extra kwetsbaarheid voor COVID-19. De Minister van Volksgezondheid, Welzijn en Sport gebruikt de geaggregeerde uitkomsten op systeemniveau, op beleidsniveau en op uitvoeringsniveau om gerichte en noodzakelijke maatregelen te treffen gericht op de volksgezondheid.
-
- **RIVM**
- 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.

-
- **Samenleving**
- Voor deelnemers is het van belang de relatie tussen Q-koorts en COVID-19 in kaart te brengen zodat eventuele risico's voor de volksgezondheid bestreden kunnen worden.

7. Verwerkingslocaties



- **Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.**
-
-
- De verwerking van alle persoonsgegevens door betrokken partijen (zie onderdeel 6) vindt plaats in Nederland.

8. Techniek en methode van gegevensverwerking



- **Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi-)geautomatiseerde besluitvorming, profilering of big data-verwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.**
-

[Klik hier om infotekst te verbergen](#)

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

Geautomatiseerde besluitvorming

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

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

- 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.

Profilerings

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

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

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

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

Big data

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

Nieuwe technologieën

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

Er is **geen** sprake van automatische besluitvorming, profilering of big data-analyse zoals bedoeld in de AVG. Het onderzoek is namelijk niet gericht op het krijgen of bieden van inzichten ten behoeve van individuele deelnemers of groepen.

Deelnemers vullen eenmalig de vragenlijst en het deelnameformulier in. Papieren deelnameformulieren en vragenlijsten worden door de onderzoekers en/of het secretariaat van EPI in Formdesk gedigitaliseerd. Zij hebben ambtshalve een beroepsgeheim en kunnen niet bij de besloten netwerkschijf. Zij krijgen een instructie hoe om te gaan met de binnengekomen retourenveloppen met deelnameformulieren en vragenlijsten. De geretourneerde papieren deelnameformulieren en vragenlijsten voor en na digitalisatie apart van elkaar bewaard worden in een afgesloten kast bij Centrum EPI waarvan de sleutel alleen beschikbaar is voor het projectteam en het secretariaat van het Centrum EPI. Na afronding van de digitalisatie van alle deelnameformulieren en vragenlijsten en het opschonen van het vragenlijstbestand zullen deze apart van elkaar opgeslagen worden in het Centraal Archief van het RIVM en later in het Nationaal Archief in Den Haag, conform de richtlijnen die het RIVM-brede project 'COVID-19 Archiveren, Reconstrueren, Vertellen, voorbereiden op Evalueren' (C-ARVE) voor gaat schrijven. Deelnemers krijgen drie weken de tijd om de vragenlijst in te vullen. De ingevulde vragenlijsten worden iedere werkdag uit Formdesk geëxporteerd naar Excel, opgeslagen op de netwerkschijf in de projectmap met beperkte toegang (enkel het projectteam) en vervolgens uit Formdesk verwijderd. Datzelfde geldt voor de ingevulde digitale gegevens uit de deelnameformulieren, deze worden iedere werkdag uit Formdesk geëxporteerd naar Excel en worden gescheiden van de vragenlijsten opgeslagen op de netwerkschijf in de projectmap met beperkte toegang (enkel het projectteam) en voorzien van encryptie en uit Formdesk verwijderd (dit gaat gelijktijdig met de vragenlijstgegevens).

-
- Het deelnemersnummer en het eventuele OSIRIS nummer van de personen die in 2020-2021 overleden zijn en waarvan een COVID-19 melding bekend is bij de GGD Hart voor Brabant worden uitgewisseld via FileSender. Na uitnodiging via email van een betrokken onderzoeker via FileSender kan de GGD Hart voor Brabant via een weblink een bestand met deelnemersnummer en OSIRIS nummer uploaden en versturen naar het RIVM. Deze verbinding verloopt via TLS (1.2). Verdere encryptie (end-to-end) wordt ingesteld door middel van een in te stellen wachtwoord op het downloaden van het bestand. De browser ver- en ontsleutelt bestanden tijdens het up- en downloaden. Dit wachtwoord wordt mondeling doorgegeven aan een van de betrokken onderzoekers. Tevens is de weblink om het bestand te kunnen uploaden maximaal 2 dagen geldig (conform het advies in **Bijlage H**).
-
- De vragenlijstgegevens worden per deelnemer gepseudonimiseerd door middel van het deelnemersnummer. De naam en andere direct identificerende gegevens (zoals ingevuld in het deelnameformulier en de adres/contactgegevens/koppelbestand van personen die toestemming geven voor eventueel toekomstig onderzoek) worden apart van de vragenlijstgegevens bewaard beveiligd met verschillende wachtwoorden dat alleen bekend is bij het projectteam en voorzien van encryptie op de netwerkschijf van het RIVM in de projectmap met beperkte toegang (alleen het projectteam). Alleen met toegang tot deze bestanden, die bij de betrokken onderzoekers blijven, zijn de vragenlijstgegevens te herleiden.
-

9. Juridisch en beleidsmatig kader



- **Benoem de wet- en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de gegevensverwerkingen.**
-

[Klik hier om infotekst te verbergen](#)

Naast of in de plaats van de AVG en de Richtlijn kan (sectorale) regelgeving de mogelijkheden voor gegevensverwerkingen creëren, conditioneren of beperken. Voorbeelden van dergelijke wetten zijn: Wet algemene bepalingen burgerservicenummer, Wet gebruik burgerservicenummer in de zorg, Wet basisregistratie personen, Algemene wet inzake rijksbelastingen, Archiefwet, Telecommunicatiewet, Kadasterwet, Handelsregisterwet 2007, Kieswet, Wet bijzondere maatregelen grootstedelijke problematiek, Wet op de geneeskundige behandelingsovereenkomst, Omgevingswet, Jeugdwet, Wet maatschappelijke ondersteuning 2015 en Participatiewet. Deze lijst is niet uitputtend.

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

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

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

- Wet publieke gezondheid;
- Besluit publieke gezondheid;
- De Wet op het RIVM (artikel 3, lid 1, sub a);
- Wet medisch-wetenschappelijk onderzoek met mensen (o.a. Artikel 1);
- Uitvoeringswet AVG;
- Archiefwet;
- Selectielijst RIVM 2004 – (Staatscourant Nr. 20886, april 2017);
- Nederlandse Gedragscode Wetenschapsbeoefening (herzien in 2014);
- Project C-ARVE.

10. Bewaartermijnen



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

[Klik hier om infotekst te verbergen](#)

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

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

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

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

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

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

De gegevens worden gedurende de wettelijk voorgeschreven termijn bewaard op het RIVM, zijnde 10 jaar. Dit is gebaseerd op de Nederlandse Gedragscode Wetenschapsbeoefening waarin is bepaald dat ter waarborging van de wetenschappelijke integriteit, transparantie en reproduceerbaarheid van het onderzoek de onderzoeksgegevens ten minste 10 jaar bewaard moeten worden.

B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel aan de hand van de feiten zoals vastgesteld in onderdeel A of de voorgenomen gegevensverwerkingen rechtmatig zijn. Het gaat hier om de beoordeling van de juridische rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen. Beoordeel tevens de wijze waarop invulling wordt gegeven aan de rechten van de betrokkenen. Voor dit onderdeel van de PIA is in het bijzonder juridische expertise nodig.

1.1. Rechtsgrond



- **Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.**
-

[Klik hier om infotekst te verbergen](#)

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

- de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
- 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;
- de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
- de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
- 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;
- 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 1.4.

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.

-
- Gebruik van de eerder verzamelde gegevens van deelnemers aan de Q-HORT studie die hebben aangegeven deel te willen nemen aan toekomstig vervolgonderzoek, wordt gebaseerd op toestemming zoals bedoeld in artikel 6 lid 1 a AVG. Ten tijde van de uitvoering van het Q-HORT onderzoek was de AVG nog niet van toepassing, wel is er in de toestemmingsverklaring uitdrukkelijk toestemming voor vervolgonderzoek op het gebied van mogelijke lange termijn effecten van Q-koorts gevraagd.
-
- De grondslag(en) voor de verwerking van verzamelde persoonsgegevens via de vragenlijsten voor deze studie is de uitvoering van taak van algemeen belang in de zin van artikel 6, eerste lid onder e AVG. Het RIVM heeft immers als taak om de ontwikkelingen op het terrein van de volksgezondheid te onderzoeken en monitoren zoals neergelegd is in artikel 3, eerste lid onder a en onder e van de Wet op het RIVM juncto artikel 6 c Wet publieke gezondheid. Dit is ook van toepassing op het samenstellen van een controlegroep welke samengesteld wordt door een (gematchte) selectie van COVID-19 meldingen uit OSIRIS te halen waarbij data minimalisatie is

toegepast op de beschikbare gepseudonimiseerde informatie in OSIRIS (zie 2.2.1). Zie voor meer details de PIA OSIRIS in **Bijlage G**.

-
- Voor de verzameling van persoonsgegevens ten behoeve van toekomstig vervolgonderzoek is de grondslag de uitdrukkelijke toestemming ingevolge artikel 6 lid 1 a AVG.

12. Bijzondere persoonsgegevens



- **Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dat is toegestaan.**

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 rechtsovereenkomst;
- 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 diagnoses, het verstrekken van gezondheidszorg 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.

-
- De grondslag voor het verwerken van de bijzondere persoonsgegevens kan gevonden worden in artikel 9, tweede lid onder g van de AVG. De verwerking is noodzakelijk voor redenen van zwaarwegend algemeen belang. Het onderzoek is noodzakelijk om te onderzoeken of Q-koorts mogelijk tot een ernstiger beloop leidt van COVID-19 (bijvoorbeeld vaker sprake van een ziekenhuis- of IC-opname) en of COVID-19 mogelijk vaker voorkomt bij personen die Q-koorts doorgemaakt hebben. Artikel 9, tweede lid onder g vereist een basis in lidstatelijk recht. Deze basis kan gevonden worden in artikel 3, eerste lid onder a en e jo. het derde lid van artikel 3 van de Wet op het RIVM, alsmede in artikel 6c Wet publieke gezondheid. Dit is ook van toepassing op het samenstellen van een controlegroep op basis van meldingen in OSIRIS.
-
- De verstrekking van medische gegevens van overleden personen vanuit de GGD Hart voor Brabant aan het RIVM vindt plaats op grond van art. 7:458 lid 1 sub a Wgbo. Het onderzoek bevat waarborgen waardoor dat de persoonlijke levenssfeer van de patiënt niet onevenredig wordt geschaad. In aanvulling op de doorbreking van het medisch beroepsgeheim geldt dat dit onderzoek een algemeen belang dient, het onderzoek zonder de beschreven gegevens niet uitgevoerd kan worden en de patiënt geen uitdrukkelijk bezwaar heeft gemaakt tegen deze verstrekking aan het RIVM (conform art. 7:458 lid 2 Wgbo). Verder speelt mee dat de GGD, als verantwoordelijke voor de medische gegevens, heeft ingeschat dat als de patiënten nog in leven zouden zijn geweest dat zij er dan geen bezwaar tegen zouden hebben wanneer het RIVM dit OSIRIS nummer ontvangt.
-

13. Doelbinding



- **Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.**

[Klik hier om infotekst te verbergen](#)

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

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

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

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

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

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

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

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

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

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

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.

- De adressen zijn tussen 2011 en 2013 door het JBZ/RIVM verzameld in het kader van de Q-HORT studie. Voor deelname aan deze studie zijn deelnemers expliciet gevraagd of zij bereid zijn deel te nemen aan vervolgonderzoek op het gebied van Q-koorts. De vraag werd als volgt gesteld op de papieren toestemmingsverklaring die de deelnemer destijds invulde: In de toekomst wordt er mogelijk nog meer wetenschappelijk onderzoek gedaan naar gevolgen van Q-koorts op de lange termijn. Gaat u ermee akkoord dat u in de toekomst nogmaals benaderd wordt voor onderzoeksdoeleinden? Vervolgens moesten één van de twee opties actief aangekruist worden: Ja, ik mag in de toekomst opnieuw benaderd worden / Nee, ik wil niet meer benaderd worden voor wetenschappelijk onderzoek. Verwerking van deze persoonsgegevens voor het onderhavige onderzoek is in lijn met het oorspronkelijke doel waarvoor ze zijn verzameld.
-
- Wat betreft het samenstellen van een controlegroep op basis van meldingen in OSIRIS, geldt het volgende. De meldingen (en gegevens) in OSIRIS zijn oorspronkelijk verzameld voor het initiële doel van vroegwaarschuwing, monitoring, surveillance en bestrijding van infectieziekten en daarmee ter bescherming van de volksgezondheid. Vervolgens kan met deze gegevens wetenschappelijk onderzoek worden uitgevoerd om meer kennis op te doen over incidentie, prevalentie en bestrijding van infectieziekten, onder andere om in de toekomst betere preventiemaatregelen te kunnen nemen. Deze verdere verwerking (in de vorm van wetenschappelijk onderzoek) is verenigbaar met het doel waarvoor de gegevens oorspronkelijk zijn verzameld (art. 5, lid 1(b) AVG en overeenkomstig art 89 lid 1 AVG).

14. Noodzaak en evenredigheid



- **Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit.**
- **a. Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?**
- **b. Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt?**
-

[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 grondrechttoets van het IAK.

-
- Het doel is om te onderzoeken of, en zo ja, welke relatie er is tussen doorgemaakte Q-koorts en extra kwetsbaarheid voor COVID-19. In onderdeel 4 is beschreven welke persoonsgegevens nodig zijn om deze relatie te onderzoeken. Hieronder wordt de proportionaliteit en subsidiariteit van deze persoonsgegevens beoordeeld.
-
- **Proportionaliteit**
- De verwerking van de persoonsgegevens is essentieel om de invloed van doorgemaakte Q-koorts op het krijgen van COVID-19 en de ernst van COVID-19 te onderzoeken. Gegevens over de gezondheid van de deelnemer, en in het bijzonder gegevens met betrekking tot de gezondheidstoestand, zijn voor dit onderzoek noodzakelijk. Het A-nummer (anoniem BSN nummer, administratief nummer van de persoon bedoeld in de Wet BRP dat is afgeleid van de BSN en is een vast nummer) is essentieel om de controle van adresgegevens in het BRP uit te voeren. Zonder deze persoonsgegevens is het feitelijk onmogelijk een onderbouwd wetenschappelijk onderzoek uit te voeren. Deelnemers verstrekken hiervoor hun gegevens pas nadat zij hierover conform de AVG zijn geïnformeerd.
-
- Dataminimalisatie wordt toegepast door alleen de gegevens te vragen die direct van invloed kunnen zijn op de uitkomsten van dit onderzoek. Verder wordt de uitvraag naar specifieke (medische) informatie zo gericht mogelijk uitgevraagd, bijvoorbeeld door eventuele symptomen en zwangerschap te beperken tot 2020 (en/of 2021 afhankelijk van wanneer verzending van de vragenlijst plaats gaat vinden) en de vragen te laten aansluiten op gegevens die ook beschikbaar zijn in OSIRIS AIZ voor COVID-19 meldingen. Ook wordt er voor de controlegroep uit OSIRIS slechts een selectie van de beschikbare informatie in OSIRIS AIZ gebruikt voor dit onderzoek.
-
- **Subsidiariteit**

- De noodzakelijke persoonsgegevens voor dit onderzoek kunnen slechts gedeeltelijk via andere wijzen verkregen worden. Zo kan de GGD benaderd worden voor testuitslagen van personen (overleden en levend) die ook Q-koorts hebben doorgemaakt. Naast juridische uitdagingen werpt dit ook de vraag op in hoeverre die informatie volledig en accuraat is, omdat aangenomen moet worden dat niet iedere deelnemer met mogelijke COVID-19 klachten zich heeft laten testen, in het bijzonder de personen die voor 1 juni 2020 klachten hadden omdat toen het COVID-19 testbeleid in Nederland nog veel strikter was. Met het huidige onderzoek kan daar door middel van extra analyses op basis van het soort klachten nog mogelijk onderscheid in gemaakt worden door verschillende de casusdefinities voor mogelijk/vermoedelijk COVID-19 te gebruiken en uitkomsten onderling te vergelijken.
- Daarnaast vormt de huidige methode van uitvragen van informatie de deelnemer de meeste 'controle' over de gegevens die in het kader van dit onderzoek gebruikt worden. De deelnemer moet immers toestemming geven voor het onderzoek, en zonder deze toestemming mogen diens gegevens niet gebruikt worden. Wordt op een andere wijze geprobeerd persoonsgegevens te verkrijgen (bijv. via de GGD), dan heeft dit in de praktijk tot gevolg dat een deelnemer mogelijk verrast wordt door het feit dat de gegevens zonder diens medeweten voor dit onderzoek worden gebruikt.
-

15. Rechten van de betrokkene



- **Geef aan hoe invulling wordt gegeven aan de rechten van betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzonderingen dat is toegestaan.**

[Klik hier om infotekst te verbergen](#)

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

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

- 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 verwerking van gegevens voor het onderhavige wetenschappelijke onderzoek is noodzakelijk voor de uitvoering van een taak van algemeen belang en deelname is vrijwillig. Tegelijkertijd heeft de deelnemer ten tijde van de Q-HORT studie (2011 – 2013) toestemming gegeven voor deelname aan toekomstig vervolgonderzoek door dit actief op het toestemmingsformulier aan te kruisen. Verder kan de deelnemer met het huidige onderzoek ook toestemming geven zijn gegevens te verwerken voor toekomstig onderzoek in het kader van Q-koorts en COVID-19. In beide gevallen worden de contactgegevens van de deelnemer verwerkt op grond van **toestemming**.

Betrokkenen kunnen te allen tijde hun toestemming intrekken wat betreft deelname aan toekomstige studies. In dat geval verwijdert het RIVM hen uit de lijst met contactgegevens voor toekomstige studies. Omdat het de inhoudelijke onderzoeksdata van de contactgegevens zijn losgekoppeld en worden verwerkt op basis van de taak van algemeen belang, heeft het intrekken van toestemming geen effect op de onderzoeksdata.

Betrokkenen stemmen in met de vrijwillige deelname aan het onderzoek door het tekenen van het deelnameformulier (grondslag algemeen belang). Zij kunnen die instemming intrekken. In praktijk houdt dat in dat zij stoppen met het invullen van de vragenlijst. Als betrokkenen stoppen met het invullen van de vragenlijst, worden ingevoerde gegevens uit die sessie gewist. Deze gegevens komen niet bij het RIVM terecht.

Gezien de dagelijkse export van gegevens uit Formdesk, en de gemiddelde looptijd van het uitoefenen van rechten van betrokkenen (in verband met identificatie), is de kans zo goed als nihil dat een verzoek kan worden gehonoreerd terwijl de gegevens nog in Formdesk staan. Daarna zijn ze gepseudonimiseerd, maar die het projectteam kan dit terugdraaien. In principe kan het RIVM dus invulling geven aan de rechten.

Op basis hiervan geldt het volgende:

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.

Het RIVM kiest ervoor deelnemers de mogelijkheid te geven om contactgegevens of de toestemming voor eventueel vervolgonderzoek aan te laten passen of te laten verwijderen door contact op te nemen met het RIVM (zoals beschreven in de deelnemersinformatie, **Bijlage D**). Instemming tot deelname aan het onderzoek kan ingetrokken worden zolang de analyses nog niet

uitgevoerd zijn én wanneer zij zich op een vergelijkbare manier identificeren als waarmee zij zich aanmeldden voor het onderzoek (met het deelnemersnummer).

Beperkingen van het recht op gegevenswissing

Betrokkenen kunnen het recht op gegevenswissing uitoefenen. Zij kunnen contact opnemen met het RIVM en aangeven hun instemming voor deelname aan het onderzoek in te trekken. Als zij zich op een vergelijkbare manier identificeren als waarmee zij zich aanmeldden voor het onderzoek (met het deelnemersnummer), én zolang de analyses nog niet uitgevoerd zijn, kan het RIVM op basis daarvan hun verzoek tot gegevenswissing honoreren. Als de gegevens al zijn gebruikt in analyses, worden die analyses niet opnieuw gedaan zonder de gegevens. Zij dragen dan dus nog bij aan geaggregeerde rapportages. Dit is uitgelegd in de deelnemersinformatie en het deelnameformulier (zie **Bijlage D en E**). Contactgegevens of de toestemming voor eventueel vervolgonderzoek kunnen na uitvoer van de analyses nog wel aangepast of verwijderd worden door de onderzoekers.

Indien de analyses reeds uitgevoerd zijn, zal het RIVM het verzoek tot gegevenswissing niet meer honoreren. De reden hiervoor is dat het onderzoek reproduceerbaar moet zijn en dat dit nodig is als kwaliteitscontrole op de uitgevoerde analyses. Hiervoor dienen de vragenlijstgegevens gebruikt te worden die in de oorspronkelijke analyse gebruikt zijn. Hierbij is het volgende van toepassing: 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.
 - De verwerking van persoonsgegevens voor het wetenschappelijke onderzoek wordt door het RIVM gedaan in het kader van de taak inzake de bestrijding van infectieziekte (artikel 6c Wet publieke gezondheid). Hierdoor kan geen beroep worden gedaan op 'recht van vergetelheid'.
 - **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).

Intrekken toestemming

De deelnemer heeft het recht zijn toestemming in te trekken voor zover dit betrekking heeft op het verwerken van zijn contactgegevens (adresgegevens, emailadres en telefoonnummer (deze laatste twee zijn optioneel in te vullen door de deelnemer)) voor vervolgonderzoek. Vanaf het moment van intrekking worden de gegevens niet langer voor dit doeleinde verwerkt (art. 7 lid 3 AVG).

C. Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de gegevensverwerking zoals in onderdeel A en B zijn beschreven en beoordeeld. Het gaat hierbij overigens niet om de risico's van de verwerkingsverantwoordelijke zelf.

16. Risico's



- **Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Ga hierbij in ieder geval in op:**
 - **a. welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen;**
 - **b. de oorsprong van deze gevolgen;**
 - **c. de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;**
 - **d. de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.**
-

[Klik hier om infotekst te verbergen](#)

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

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

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

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

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

1. Risico's identificeren

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

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

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

2. Risico's inschatten

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

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

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

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

De kans dat zich gevolgen voordoen voor de rechten en vrijheden van de betrokkenen, kan tevens verband

houden met de (mate van) beveiliging van de persoonsgegevens. De al dan niet opzettelijke:

- vernietiging en verlies (beschikbaarheid);
- wijziging (integriteit);
- ongeoorloofde toegang en verstrekking (vertrouwelijkheid);

van persoonsgegevens, kan leiden tot schade voor de betrokkene.

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

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

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

3. Risico's beoordelen

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

In dit onderdeel worden per datastap (zie schema in onderdeel 3) de potentiële risico's voor betrokkenen beoordeeld. De verwerkingen hebben niet tot doel enige directe impact op betrokkenen te hebben. De betrokkenen hebben geen direct belang bij de resultaten van het onderzoek en ondervinden ook geen directe gevolgen van de uitslagen van het onderzoek. In die zin hebben de gegevensverwerkingen in het kader van dit onderzoek dan ook geen impact op betrokkenen als er iets fout gaat (zie daarover algemene risico's hieronder).

De kans bestaat wel dat betrokkenen indirect gevolgen ondervinden aan dit onderzoek, bijvoorbeeld als de uitkomsten van het onderzoek (samen met de andere deelonderzoeken) aanwijzingen geven voor ernstiger verloop van COVID-19 onder personen met doorgemaakte Q-koorts, waar vervolgens actief of preventief beleid op wordt gevoerd door de overheid. Ten eerste valt die mogelijkheid buiten de scope van deze DPIA, omdat het geen gevolg is van de gegevensverwerking, maar van het beleid dat erop volgt. En ten tweede stemmen personen zelf in met deelname aan het onderzoek.

Het is wel relevant om te benoemen dat het onderzoek kan bijdragen aan onterechte negatieve impact op betrokkenen, als er met foutieve gegevens wordt gewerkt of er onterechte conclusies worden getrokken. De kans dat deze impact ontstaat is klein, omdat het een onwaarschijnlijke samenloop van verschillende omstandigheden vergt en omdat het RIVM maatregelen neemt om juiste gegevens op de juiste wijze te verwerken.

Algemene risico's

Naast risico's die specifiek voor een processtap gelden, zijn er een aantal risico's die op meerdere of zelfs alle processtappen van toepassing zijn. Die kunnen zich voordoen als in dit onderzoek niet volgens de wettelijke kaders en RIVM-protocollen wordt gewerkt. Voorbeelden zijn beveiligingsincidenten/datalekken, bewaartermijnoverschrijdingen, onrechtmatige verdere verwerking van persoonsgegevens. Die risico's zijn inherent aan elke gegevensverwerking en dus elke processtap. Samen met de risico's per processtap zijn hiervoor in onderdeel D passende maatregelen beschreven.

-
-
-

Stap 1: verzamelen adresgegevens deelnemers Q-HORT

- Hier is het risico voor betrokkenen dat zij aan de lijst met deelnemers worden toegevoegd, terwijl zij hiervoor geen toestemming hebben gegeven. Dit kan de deelnemer (na uitnodiging in stap 3 en 4) een gevoel van onbehagen en verlies van controle over de persoonsgegevens geven.

-

Stap 2: Actualisatie adresgegevens deelnemers Q-HORT en controle melding COVID-19 bij overleden deelnemers

- Hier bestaat het risico dat de persoonsgegevens door een onbevoegd persoon worden ontvangen, of worden onderschept. Inzage in de persoonsgegevens is dan – althans in theorie – mogelijk.
- Voor de actualisatie van de adresgegevens wordt gebruik gemaakt van een webservice van de firma T&T (vertrouwdverbonden.nl) (*Bijlage H*). De uitwisseling van de (geactualiseerde) adresgegevens zijn kwetsbaar voor een datalek. T&T biedt de resultaten aan via hun webapplicatie, en die blijven daar ca. een maand voor klaarstaan. T&T zelf heeft vermoedelijk altijd toegang tot alle persoonsgegevens van Nederland, ze beheren deze immers. De webapplicatie is zeer goed beveiligd, door een combinatie van gebruikersnaam, wachtwoord, bekend IP-adres en browser-certificaat.
- Dit is bekend over de beveiliging: Vanuit T&T wordt een adres (url) verstrekt waarmee de applicatie in een browser kan worden gestart. Dit is alleen mogelijk als:

- Het IP-adres van de afnemer bekend is op de firewall bij T&T;
- De gebruiker de certificaten heeft geïnstalleerd in de browser.
- Na het starten verschijnt het inlogscherf waarop de gebruikersnaam en het wachtwoord kunnen worden ingegeven. Als deze correct zijn ingegeven kan de gebruiker via de tabbladen bovenaan het scherm en de knoppen links in het scherm een keuze maken voor een functie. De tabbladen en menukeuzes die worden getoond zijn afhankelijk van de autorisatie van een gebruiker.
- De beheerder van de applicatie (die inlogt onder de gereserveerde naam beheerder) krijgt na het inloggen een blanco scherm en moet zelf met behulp van de tabbladen en het menu een initiële keuze maken. Alle overige gebruikers komen in het scherm terecht voor het stellen van een vraag (tab Vragen, knop vraag onder het kopje GBA-V LO3).
- Dit is bekend over het certificaat: Het certificaatwachtwoord ten behoeve van de GBA-V LO3 bevraging mag niet worden opgeslagen. Wanneer een nieuwe versie van de programmatuur geïnstalleerd is, dient T&T eenmalig het certificaatwachtwoord in te brengen. Daarna kan er pas een GBA-V LO3 vraag gesteld worden. Indien het certificaatwachtwoord nog niet ingegeven is en men gaat een GBA-V LO3 vraag stellen, verschijnt de foutmelding "T&T dient het certificaatwachtwoord in te brengen".

-

- De verstrekking van gegevens van overleden deelnemers vanuit GGD Hart voor Brabant kent geen risico's voor de betrokkene, aangezien die immers overleden zijn. Wel is in het kader van het medisch beroepsgeheim van belang te bepalen of de betrokkene bij leven zijn toestemming heeft verleend voor verstrekking van zijn gegevens voor dit onderzoek, of dat er conform art. 7:458 Wgbo een uitzondering van toepassing is. GGD Hart voor Brabant is de verantwoordelijke voor deze gegevens en voert deze beoordeling uit. Verstrekking van deze gegevens gebeurt digitaal, en dient gezien de aard van de gegevens op een voldoende veilige methode plaats te vinden. Indien verstrekking mogelijk is, dan dienen partijen aanvullende waarborgen in een Data Sharing Agreement (**Bijlage J**) te beschrijven (de versie in de bijlage is goedgekeurd namens het RIVM en is naar de GGD Hart voor Brabant gestuurd ter controle/ondertekening).
-
- **Stap 3 en 4: Uitnodiging versturen, verzamelen documenten en vastleggen toestemming vervolgonderzoek**
- Hier bestaat het risico dat deelnemers worden uitgenodigd die geen toestemming hebben gegeven, of ondanks eerdere toestemming alsnog niet willen deelnemen aan het onderhavige vervolgonderzoek. Dit kan veroorzaakt worden door het feit dat toestemming voor vervolgonderzoek tussen 2011 – 2013 is verstrekt en de deelnemer dit was vergeten. Ook kunnen mogelijke deelnemers 'overvallen' worden door het verzoek. Dit kan ertoe leiden dat deelnemers geconfronteerd worden herinneringen aan de ziekteperiode met Q-koorts en de vervelende gevolgen die dit toentertijd voor de deelnemer heeft gehad.
-

Verder worden de digitale formulieren in Formdesk verwerkt. Hiervoor is geen noemenswaardige negatieve impact te bedenken voor betrokkenen die kan volgen uit het verwerken van gebruiksgegevens in Formdesk door het RIVM. De ingevulde vragenlijstgegevens worden pas helemaal op het eind opgeslagen wanneer de deelnemer op 'Verzenden' klikt. Indien hij/zij tijdens het invullen van de vragenlijst wil stoppen, dan kan dat zonder en de tot dusver ingevulde gegevens staan niet in Formdesk. Het kan voorkomen dat iemand ervoor kiest om deel te nemen aan het onderzoek, spijt krijgt en niet meer wil deelnemen. De persoon kan na verzenden zelf niet meer bij het vragenformulier, maar hij/zij kan wel contact opnemen met de onderzoekers om de gegevens alsnog te laten wissen zolang als de analyses nog niet uitgevoerd zijn (uitgelegd in **Bijlage D**). Toestemming voor eventueel nieuw vervolgonderzoek kan altijd nog ingetrokken worden of contactgegevens laten wijzigen kan zolang als de gegevens bewaard zijn.

Papieren formulieren (deelnameformulieren en vragenlijsten) worden door het secretariaat van EPI en/of de betrokken onderzoekers handmatig ingevoerd in Formdesk. Deze handelingen kunnen ervoor zorgen dat er verkeerde gegevens ingevoerd. De deelnameformulieren en vragenlijsten worden gescheiden van elkaar voor controle bewaard (eerst in het Centraal Archief van het RIVM en later in het Nationaal Archief in Den Haag, conform de richtlijnen die Project C-ARVE voor gaat schrijven). De kans bestaat dat deze gegevens door een derde geraadpleegd kunnen worden.

Ondanks de dagelijkse export (ma t/m vr) van ingevulde gegevens vanuit Formdesk, bestaat het risico dat een export niet goed plaatsvindt. In dat geval blijven gegevens achter op de server van Formdesk, wat er mogelijk toe kan leiden dat de controle over de persoonsgegevens verloren raakt. Aan de andere kant blijven gegevens nu niet onnodig lang bewaard in Formdesk maar worden ze regelmatig opgeslagen op een afgeschermd locatie op de netwerkschijf van het RIVM waar alleen het projectteam toegang toe heeft. Formdesk zorgt voor een back-up van de aanwezige gegevens. Dit proces verloopt automatisch. De gegevens worden maximaal 1 maand bewaard. Daarna worden ze automatisch gewist. In theorie zou een select groepje databasebeheerders van Innovero (aanbieder Formdesk) toegang kunnen krijgen tot de RIVM gegevens in de betreffende databases.

- **Stap 5: Aanmaken controlegroep**

- Op basis van meldingen in OSIRIS AIZ wordt een controlegroep aangemaakt. Volgens de PIA OSIRIS-AIZ (maart 2020, **Bijlage G**) bestaan enkele risico's bij de registratie van meldingen in OSIRIS AIZ. Deze risico's zijn echter in het kader van de controlegroep niet van toepassing, omdat de controlegroep op basis van gepseudonimiseerde gegevens (sleutel bij de GGD) wordt samengesteld. Hiervoor is herleidbare informatie niet nodig of gewenst, maar slechts informatie over besmetting met COVID-19, de symptomen en het verloop. Omdat de meldingen in OSIRIS AIZ aan de bron zijn gepseudonimiseerd, is voor betrokkenen geen noemenswaardig risico te benoemen.
-
- **Stap 6: Uitvoeren wetenschappelijk onderzoek**
- Er wordt slechts gewerkt met gepseudonimiseerde gegevens (er zal een gecombineerde dataset gemaakt worden van de gepseudonimiseerde vragenlijstgegevens en de gepseudonimiseerde gegevens uit OSIRIS voor de personen met doorgemaakte Q-koorts die overleden zijn en de controlegroep om de data-analyses uit te voeren). Toegang tot de gegevens van dit onderzoek is voorbehouden aan de direct betrokken onderzoekers. Rapportage en toelichting van de bevindingen vindt slechts op geaggregeerd niveau plaats waarbij geen enkele herleidbaarheid tot een individu mogelijk is. In de uitvoering van dit onderzoek is daarom geen noemenswaardig risico voor betrokkenen te benoemen. Op verzoek van VWS zal er een publicatie geschreven worden over de resultaten. Mogelijk wordt er ook nog een wetenschappelijk artikel geschreven. Indien het voor publicatie van het artikel nodig is om de onderzoeksgegevens vrij te geven dan zal de dataset met vragenlijstgegevens eerst geanonimiseerd worden zodat deze niet meer herleidbaar is.

D. Beschrijving voorgenomen maatregelen

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

17. Maatregelen



- **Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.**

[Klik hier om infotekst te verbergen](#)

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

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

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

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

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

Ter illustratie noemt de AVG de volgende maatregelen:

- 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. gebruikscntrole
- e. controle op de toegang tot gegevens;
- f. transmissiecontrole;
- g. invoercontrole;
- h. transportcontrole; en
- i. herstelbaarheid.

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

van die persoonsgegevens.

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

Big Data

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

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

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

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

Op basis van de risico's in onderdeel C worden hieronder de maatregelen beschreven die deze risico's voorkomen of verminderen. Per processtap worden verschillende maatregelen genomen om verschillende risico's te mitigeren. Het basisbeveiligingsniveau (BBN) van de Q-koorts en COVID-19 studie is in kaart gebracht door middel van de Quickscan Information Security (QIS), kortweg Quickscan BIO (*Bijlage K*).

Stap 1: verzamelen adresgegevens deelnemers Q-HORT

Het adressenbestand dat opgeslagen is bij het JBZ wordt versleuteld verzonden naar 5.1.2e 5.1.2e. Volgens het goedgekeurde METC protocol van het Q-HORT onderzoek heeft 5.1.2e toegang tot dit bestand. Voor de verzending van het adresbestand vanuit JBZ aan het RIVM wordt gebruik gemaakt van FileSender. Dit is een centraal door het RIVM gebruikte en via SURF geleverde dienst. Er bestaat een verwerkersovereenkomst tussen het RIVM en SURF voor deze dienst. De website filesender.rivm.nl wordt hiervoor gebruikt. Inloggen op de website kan alleen met een persoonlijke RIVM-gebruikersnaam en -wachtwoord.

Na een uitnodiging via email kan via een weblink een bestand worden gedownload of geüpload (via een TLS (1.2)-verbinding). Dit kan alleen gestart worden door in te loggen met een RIVM-account (dus geen aparte inlognaam/wachtwoord). Er wordt bij inloggen geen aparte twee-factor authenticatie gebruikt. Dit is geen bezwaar zolang de encryptie-optie is gebruikt.

De uitwisseling van persoonsgegevens vindt plaats door een zogenaamde 'voucher' te sturen naar een derde partij (bijvoorbeeld JbZ), waarmee ze eenmalig een (encrypted) bestand kunnen klaarzetten voor download door RIVM.

Voor gebruik van FileSender voor dit onderzoek gelden wel de volgende voorwaarden:

- De optie 'Encryptie' moet ALTIJD gebruikt worden bij delen van bestanden.
- De geldigheid van de downloadlink moet zo gezet worden dat deze gedurende de volgende 2 werkdagen gebruikt kan worden (standaard is dit een periode van 14 dagen).

Verdere beveiliging wordt ingesteld door middel van een wachtwoord op het downloaden van het bestand (onderdeel van de encryptie optie). Dit wachtwoord wordt mondeling doorgegeven door het JbZ aan **5.1.2e** **5.1.2e**. Na ontvangst bepaalt **5.1.2e** wie van de deelnemers toestemming heeft gegeven voor vervolgonderzoek en slaat alleen de adresgegevens van deze personen op. Daarna wordt dit bestand met oude adresgegevens van personen die toestemming hebben gegeven versleuteld met een wachtwoord en voorzien van encryptie opgeslagen op de netwerkschijf van het RIVM in een map die alleen toegankelijk is voor het projectteam. Het wachtwoord voor dit bestand is alleen bekend bij het projectteam en de data-analist van de afdeling RDG.

Stap 2: Actualisatie adresgegevens deelnemers Q-HORT en controle melding COVID-19 bij overleden deelnemers

Aansluitend wordt het adresbestand van Q-HORT deelnemers die toestemming hebben gegeven voor vervolgonderzoek door het projectteam (beveiligd met een wachtwoord) intern opgestuurd naar een data-analist van het RIVM/SSC Campus, afdeling RDG om de gedateerde adresgegevens te actualiseren en te controleren of personen overleden of geëmigreerd zijn. Het wachtwoord wordt mondeling door een lid van het projectteam doorgegeven aan een data-analist van de afdeling RDG. Dit bestand wordt voor de duur van dit onderzoek opgeslagen binnen de BRP/GBA-projectmap op de RIVM netwerkschijf (waar in totaal 8 collega's van SSC Campus toegang toe hebben) en wordt naast een wachtwoord ook voorzien van encryptie.

De BRP controle vindt plaats via de firma T&T. Voor het RIVM is een eigen GBA-koppeling ingericht op de servers van T&T. Middels certificaten wordt veiliggesteld dat alleen de afnemer toegang kan krijgen tot zijn eigen GBA-omgeving, terwijl de gehanteerde TLS (1.2)-beveiliging van het internetverkeer ervoor zorgt dat de privacygevoelige informatie cryptografisch beveiligd over het internet wordt verstuurd. De gehanteerde beveiligingsmechanismen zijn dezelfde als die binnen het reguliere GBA-berichtenverkeer worden gehanteerd. Verder is er een verwerkersovereenkomst tussen het RIVM en T&T.

De controle in het BRP werkt als volgt. Bij deze webservice wordt door de data-analist een bestand met identificerende persoonsdata (naam, geslacht en geboortedatum) van de Q-HORT deelnemers geüpload. Na enkele uren wordt door de webservice een xml-bestand geproduceerd met de volledige adresgegevens en A-nummers (anoniem BSN nummer, administratief nummer van de persoon bedoeld in de Wet BRP dat is afgeleid van de BSN en is een vast nummer) terug van alle personen die daaraan voldoen, dat kan dus per deelnemer tot meerdere treffers leiden. Hij zoekt dan uit welk adres (van dat moment) en A-nummer bij de deelnemers hoort. De tweede upload volgt een aantal dagen/ weken later en bevat alleen het A-nummer (anoniem BSN) van alleen de deelnemers om nogmaals het laatste bekende adres te achterhalen. Het resultaat is het volledige en actuele adres van de deelnemers, inclusief eventueel moment van overlijden of emigratie. Deze adresgegevens zullen uiteindelijk gebruikt worden om de deelnemers aan te schrijven. De data-analist van de afdeling RDG0 voert deze BRP controle uit volgens de RIVM-regels en gebruikt hiervoor BRP gegevens voor die nodig zijn om tot de juiste adressering te komen. Het geactualiseerde bestand, inclusief de personen die in 2020-2021 overleden zijn, wordt beveiligd met

een wachtwoord en per email verstuurd naar het projectteam (Interne RIVM email is beveiligd). Vervolgens wordt het bestand versleuteld met een wachtwoord en voorzien van encryptie opgeslagen op de netwerkschijf van het RIVM in een map die alleen toegankelijk is voor het projectteam (momenteel 4 personen). Het bestand met de geactualiseerde adresgegevens dat de data-analist samengesteld heeft, wordt verwijderd uit de BRP/GBA-projectmap na ontvangst van dit bestand door het projectteam.

- De webapplicatie van T&T is zeer goed beveiligd, door een combinatie van gebruikersnaam, wachtwoord, bekend IP-adres en browser-certificaat.
- Dit is bekend over de beveiliging: Vanuit T&T wordt een adres (url) verstrekt waarmee de applicatie in een browser kan worden gestart. Dit is alleen mogelijk als:
- Het IP-adres van de afnemer bekend is op de firewall bij T&T;
- De gebruiker de certificaten heeft geïnstalleerd in de browser.
- Na het starten verschijnt het inlogscherf waarop de gebruikersnaam en het wachtwoord kunnen worden ingegeven. Als deze correct zijn ingegeven kan de gebruiker via de tabbladen bovenaan het scherm en de knoppen links in het scherm een keuze maken voor een functie. De tabbladen en menukeuzes die worden getoond zijn afhankelijk van de autorisatie van een gebruiker.
- De beheerder van de applicatie (die inlogt onder de gereserveerde naam beheerder) krijgt na het inloggen een blanco scherm en moet zelf met behulp van de tabbladen en het menu een initiële keuze maken. Alle overige gebruikers komen in het scherm terecht voor het stellen van een vraag (tab Vragen, knop vraag onder het kopje GBA-V LO3).
- Dit is bekend over het certificaat: Het certificaatwachtwoord ten behoeve van de GBA-V LO3 bevraging mag niet worden opgeslagen. Wanneer een nieuwe versie van de programmatuur geïnstalleerd is, dient T&T eenmalig het certificaatwachtwoord in te brengen. Daarna kan er pas een GBA-V LO3 vraag gesteld worden.
- Indien het certificaatwachtwoord nog niet ingegeven is en men gaat een GBA-V LO3 vraag stellen, verschijnt de foutmelding "T&T dient het certificaatwachtwoord in te brengen".

Op basis van deze werkwijze is (zie Bijlage H en I) geconcludeerd dat voor het gebruik van deze webservice van T&T geen aanvullende maatregelen nodig zijn.

GGD Hart voor Brabant is de verantwoordelijke voor de medische gegevens van overleden deelnemers en heeft beoordeeld dat verstrekking op grond van art. 7:458 Wgbo is toegestaan. Verstrekking van deze gegevens gebeurt digitaal, en dient gezien de aard van de gegevens op een voldoende veilige methode plaats te vinden. Ter verduidelijking sluiten het RIVM en de GGD hiervoor een *Data Sharing Agreement (Bijlage J)* (de versie in de bijlage is goedgekeurd namens het RIVM en is naar de GGD Hart voor Brabant gestuurd ter controle/ondertekening). Het digitale bestand voor GGD Hart voor Brabant met overleden personen die de GGD gaat controleren op gemeld zijn als overleden met/door COVID-19 wordt versleuteld met een wachtwoord en voorzien van encryptie opgeslagen op de netwerkschijf van het RIVM in een map die alleen toegankelijk is voor het projectteam (momenteel 4 personen). Het wachtwoord om dit bestand te openen staat vermeld in een ander document dat opgeslagen is in een map op de netwerkschijf van het RIVM die alleen toegankelijk is voor de betrokken onderzoekers. Het bestand zal door een lid van het projectteam met behulp van FileSender versleuteld naar de GGD Hart voor Brabant gestuurd worden en FileSender wordt ook gebruikt om het bestand met het deelnemersnummer en OSIRIS AIZ nummer retour te krijgen:

- Vanuit het RIVM wordt een encrypted bestand klaargezet voor download (van toepassing op het verzenden van het databestand van overleden personen van het RIVM naar GGD Hart voor Brabant), geldigheid om te downloaden 2 werkdagen;
- Er wordt een zogenaamde 'voucher' gestuurd naar een derde partij (GGD Hart voor Brabant), waarmee ze eenmalig een (encrypted) bestand kunnen klaarzetten voor

download door RIVM (van toepassing op de verzending van GGD Hart voor Brabant naar RIVM), geldigheid om te uploaden 2 werkdagen.

Stap 3 en 4: Uitnodiging versturen, verzamelen documenten en vastleggen toestemming vervolgonderzoek

Na actualisatie van de adresgegevens ontvangen de deelnemers aan de studie een envelop met een korte uitnodigingsbrief met adresgegevens, de uitgebreide deelnemersinformatie (**Bijlage D**), twee deelnameformulieren (**Bijlage E**), een vragenlijst (**Bijlage F**) en een retourenvelop (met de vermelding 'VERTROUWELIJK' erop). Zij hebben de keus om deze documenten schriftelijk of digitaal via Formdesk in te vullen (zie ook **Bijlage D en H**). Formdesk is nu in totaal drie keer onderwerp geweest van een penetratietest (uitgevoerd in opdracht van het RIVM, waarvan twee zijn uitgevoerd na het bewuste incident). Hieruit zijn geen 'show stoppers' naar voren gekomen. Formdesk laat zelf ook regelmatig pentests uitvoeren op hun dienst. Daarnaast is er na het incident opnieuw een uitgebreide risicoanalyse uitgevoerd, waarbij de conclusie was dat Formdesk als oplossing door het RIVM ingezet kan worden voor het ondersteunen van onderzoeken. De kwetsbaarheid (URL tampering) die ten grondslag lag aan het incident met Infectieradar is hier niet van toepassing, omdat de vragenlijsten maar éénmalig ingevuld kunnen worden. Verder zorgt Formdesk voor een automatische back-up van de aanwezige gegevens. Deze gegevens worden maximaal één maand bewaard. Daarna worden ze automatisch gewist. Formdesk past daarnaast een encrypted verbinding toe op de gegevens die uitgewisseld worden (**Bijlage H en I**). De meest 'recente' Quickscan van Formdesk is uit 2019, maar deze is nog steeds relevant (**Bijlage L**). Indien deelnemers kiezen voor het digitaal invoeren van de vragenlijst dan vullen zij ook het deelnameformulier digitaal in (toestemming moet uitdrukkelijk zijn verleend met een extra vinkje voordat de vragenlijst ingevuld en verzonden kan worden).

De geretoureerde papieren deelnameformulieren en vragenlijsten zullen voor en na digitalisatie apart van elkaar bewaard worden in een afgesloten kast bij Centrum EPI (sleutel alleen beschikbaar voor het projectteam en het secretariaat van het Centrum EPI). Dit is nodig om de onderzoeksgegevens bij een vermoeden van fouten na digitalisatie te controleren. Digitalisatie van de papieren vragenlijsten gebeurt door het secretariaat van EPI en/of de betrokken onderzoekers via Formdesk. Zij hebben ambtshalve een beroepsgeheim. Na afronding van de digitalisatie van alle deelnameformulieren en vragenlijsten en het opschonen van het vragenlijstbestand zullen deze apart van elkaar opgeslagen worden in het Centraal Archief van het RIVM. Na maximaal 20 jaren gaan deze naar het Nationaal Archief in Den Haag. Tevens zullen de richtlijnen gevolgd worden die door het RIVM-brede project C-ARVE voorgeschreven worden. Dit zorgt ervoor dat het RIVM organisatiebreed alle adviezen, rapporten, maar ook alle mails en digitale berichten over COVID-19 zorgvuldig archiveert.

De Formdesk beheer omgeving is alleen beschikbaar via Campus Pro werkplek (beveiligde RIVM-netwerk) op basis van de persoonlijke RIVM gebruikersnaam en wachtwoord (alleen beschikbaar voor medewerkers). In geval van inloggen in Campus buiten het RIVM wordt gebruik gemaakt van 2 factor-authenticatie. Beschikbaarheid van onderzoeksgegevens is beperkt tot de rechtstreeks betrokken onderzoekers van het RIVM. Dagelijks van maandag tot en met vrijdag worden de ingevulde vragenlijsten uit Formdesk geëxporteerd. Na de export worden de ingevulde gegevens in het deelnameformulier (plus het deelnemersnummer) in een apart Excel bestand opgeslagen en de vragenlijstgegevens (plus het deelnemersnummer) in een apart Excel bestand. Beide bestanden worden opgeslagen op de netwerkschijf in de projectmap met beperkte toegang (enkel het projectteam) en vervolgens uit Formdesk verwijderd. De bestanden met de gegevens uit de deelnameformulieren worden daarnaast beveiligd met een wachtwoord en voorzien van encryptie. Na afronding van de invoer van alle vragenlijsten zal er van de losse Excel vragenlijstbestanden één bestand gemaakt worden met alle gegevens erin en hetzelfde wordt gedaan voor alle Excel deelnameformulier bestanden. Deze worden op in dezelfde map opgeslagen en op dezelfde manier

beveiligd als de losse bestanden. FormDesk zorgt voor een back-up van de aanwezige gegevens. Dit proces verloopt automatisch. De gegevens worden maximaal 1 maand bewaard. Daarna worden ze automatisch gewist.

Het digitale bestand met de vragenlijstgegevens is gepseudonimiseerd (op basis van het 4-cijferige deelnemersnummer) en zonder toegang tot het bestand met deelnameformulieren of adresbestand is er geen mogelijkheid om deze gegevens aan elkaar te koppelen (deze zijn voorzien van encryptie en een wachtwoord opgeslagen op de RIVM-netwerkschijf in een map die alleen toegankelijk is voor de betrokken onderzoekers). Het wachtwoord om het bestand met deelnameformulieren of adresbestand te openen staat vermeld in een ander document dat opgeslagen is in een map op de netwerkschijf van het RIVM die alleen toegankelijk is voor de betrokken onderzoekers. Op basis van de beschreven werkwijze is geconcludeerd dat voor het gebruik van Formdesk geen aanvullende twee-factor-authenticatie nodig is (zie **Bijlage H**).

Het digitale bestand met de adresgegevens (plus eventueel het optioneel ingevulde emailadres en telefoonnummer) van deelnemers die via het huidige onderzoek toestemming hebben gegeven voor deelname aan nieuw vervolgonderzoek naar Q-koorts en COVID-19 zal versleuteld met een wachtwoord en voorzien van encryptie opgeslagen worden op de netwerkschijf van het RIVM in een map die alleen toegankelijk is voor het projectteam. Deze gegevens zijn zonder toegang tot dit bestand niet te koppelen aan de gepseudonimiseerde gegevens uit de vragenlijsten. Het wachtwoord om het adresbestand 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 de betrokken onderzoekers. Deelnemers geven op het deelnameformulier aan of ze toestemming geven voor eventueel vervolgonderzoek. Deze deelnameformulieren worden apart bewaard (op papier en digitaal) van de vragenlijstgegevens. Om een adresbestand te maken van de deelnemers die toestemming hebben gegeven is alleen een tijdelijke koppeling nodig tussen het geactualiseerde adresbestand en het deelnameformulier en niet met de vragenlijst.

Stap 5: Aanmaken controlegroep

Voor het aanmaken van een controlegroep van COVID-19 meldingen wordt een selectie in OSIRIS AIZ gemaakt. Dit zijn in alle gevallen persoonsgegevens die aan de bron zijn gepseudonimiseerd. De sleutel hiervan wordt in dit geval bewaard door de GGD, waardoor herleidbaarheid door het RIVM in redelijkheid niet mogelijk is. De risicoanalyse/quickscan en PEN-test voor OSIRIS AIZ zijn uitgevoerd.

Stap 6: Uitvoeren wetenschappelijk onderzoek

Analyse van de gegevens gebeurt op basis van de gepseudonimiseerde gegevens. Voor de analyse wordt gebruik gemaakt van Excel en SAS/SPSS/R/STATA. Deze bestanden bevatten dus alleen gepseudonimiseerde persoonsgegevens opgeslagen op de netwerkschijf van het RIVM in een map die alleen toegankelijk is voor het projectteam.

- Verder kunnen deelnemers aangegeven dat zij op de hoogte worden gesteld van de geaggregeerde uitkomsten uit dit onderzoek per email. Onderzoekresultaten die gepubliceerd worden, zijn samengesteld op basis van de analyse van de gegevens en zijn op geaggregeerd niveau. De publicatie (voor VWS en mogelijk een wetenschappelijk artikel) vindt plaats op geaggregeerd niveau en zonder herleidbare persoonsgegevens. Indien het voor de wetenschappelijke publicatie nodig is om de onderzoeksgegevens vrij te geven dan zal de dataset met vragenlijstgegevens eerst geanonimiseerd worden zodat deze niet meer herleidbaar is.

Algemene maatregelen

1. Het basisbeveiligingsniveau (BBN) van de Q-koorts en COVID-19 studie is in kaart gebracht door middel van de Quickscan Information Security (QIS), kortweg Quickscan BIO (*Bijlage K*);
2. Toegang tot databestanden alleen voor de direct betrokken onderzoekers: bestanden met contactgegevens en het koppelbestand beveiligd door middel van wachtwoorden en voorzien van encryptie;
3. Computer op lock zetten bij afwezigheid;
4. 2 factor-authenticatie in geval van inloggen in Campus buiten het RIVM;
5. Regelmatige controle op wie toegang heeft tot de onderzoeksdata;
6. Back-up van de RIVM-netwerkschijf enkele keren per dag. Wanneer iets per ongeluk verwijderd is, is dit terug te halen met behulp van de back-up.

VWS, RIVM, CIB, EPI, RES - Q-koorts en COVID-19 (deelonderzoek 2, Q-HORT en COVID-19)

Bijlagen

Bijlage A. Definitieve COVID-19 en Q-koorts onderzoeksvoorstel

Bijlage B. Kamerbrief stand van zaken COVID-19 van 21 september 2020 (Kamerstuk 25 295, nr 534)

Bijlage C. Opdrachtbrief VWS voor onderzoek Q-koorts en COVID-19

Bijlage D. Deelnemersinformatie Q-koorts (Q-HORT) en COVID-19 onderzoek, versie 6, 12-11-2020

Bijlage E. Deelname- en toestemmingsformulier Q-koorts (Q-HORT) en COVID-19 onderzoek, versie 6, 12-11-2020

Bijlage F. Vragenlijst Q-koorts (Q-HORT) en COVID-19 onderzoek, versie 6, 12-11-2020

Bijlage G. PIA OSIRIS AIZ, versie 2, maart 2020

Bijlage H. Analyse Informatiebeveiliging Q-koorts COVID-19 obv Formdesk-FileSender 201028

Bijlage I. Systeemdecompositie - Q-koorts COVID-19 obv Formdesk-FileSender 201028

Bijlage J. Data Sharing Agreement met GGD HvB, versie 4

Bijlage K. Quickscan Q-koorts COVID-19 onderzoek versie 1.0

Bijlage L. Quickscan (QIS) Formdesk Algemeen 190430

•



Maatregelen
nemen
Privacybewustwording
Doelbinding
PIA
Noodzaak
Effecten in kaart
Bescherming van
persoonsgegevens
Risico's
minimaliseren
Richtinggevend
Rechtsgrond
Met open vizier