

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst

**GEZAMENLIJKE VERWERKINGSVERANTWOORDELIJKEN
OVEREENKOMST**

Project: CONTROL: effectiviteit & optimalisatie van bron- en contactonderzoek om de verspreiding van SARS-CoV-2 te beperken

Partijen

1. Gemeente Amsterdam, directie Geneeskundige en Gezondheidsdienst Amsterdam, gevestigd te Amsterdam aan de Nieuwe Achtergracht 100, ingeschreven in het handelsregister onder KvK nummer KvK 34366966, hierna te noemen "**GGD Amsterdam**", rechtsgeldig vertegenwoordigd door 5.1.2e 5.1.2e;
2. De Gemeentelijke Gezondheidsdienst GGD Flevoland, gevestigd te Lelystad aan de Noorderwagenstraat 2, ingeschreven in het handelsregister onder KvK nummer 32170511, hierna te noemen "**GGD Flevoland**", rechtsgeldig vertegenwoordigd door 5.1.2e
3. De Veiligheids- en Gezondheidsregio Gelderland-Midden, gevestigd te Arnhem aan de Eusebiusbuitensingel 43, ingeschreven in het handelsregister onder KvK nummer 09217053, hierna te noemen "**GGD Gelderland-Midden**", rechtsgeldig vertegenwoordigd door 5.1.2e 5.1.2e
4. De Gemeentelijke Gezondheidsdienst GGD Groningen, gevestigd te Groningen aan het Hanzeplein 120, ingeschreven in het handelsregister onder KvK nummer 62089781, hierna te noemen "**GGD Groningen**", rechtsgeldig vertegenwoordigd door 5.1.2e
5. De Gemeentelijke Gezondheidsdienst Hart voor Brabant, gevestigd te 's-Hertogenbosch aan de Pettelaarpark 10, ingeschreven in het handelsregister onder KvK nummer 17247544, hierna te noemen "**GGD Hart voor Brabant**", rechtsgeldig vertegenwoordigd door 5.1.2e
6. De Gemeentelijke Gezondheidsdienst GGD Regio Utrecht, gevestigd te Zeist aan de Dreef 5, ingeschreven in het handelsregister onder KvK nummer 50909185, hierna te noemen "**GGD Regio Utrecht**", rechtsgeldig vertegenwoordigd door 5.1.2e
7. Gemeente Rotterdam, als uitvoerende gemeente voor de Gemeentelijke Gezondheidsdienst Rotterdam-Rijnmond gevestigd te Rotterdam aan de Schiedamsedijk 95, ingeschreven in het handelsregister onder KvK nummer 24483298, hierna te noemen "**GGD Rotterdam-Rijnmond**", rechtsgeldig vertegenwoordigd door 5.1.2e
8. De Geneeskundige Gezondheidsdienst Zuid-Limburg, gevestigd te Heerlen aan het Overloon 2, ingeschreven in het handelsregister onder KvK nummer 14131474, hierna te noemen "**GGD Zuid-Limburg**", rechtsgeldig vertegenwoordigd door 5.1.2e

Gezamenlijk verder te noemen "Partijen" en individueel 'Partij'.

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst

in aanmerking nemende dat:

- Partijen in het kader van het in Bijlage 1 gespecificeerde project wensen samen te werken;
- Partijen voor deze samenwerking op 1 oktober 2020 een Hoofdovereenkomst hebben gesloten met titel 'SAMENWERKINGSOVEREENKOMST Project: CONTROL: effectiviteit & optimalisatie van bron- en contactonderzoek om de verspreiding van SARS-CoV-2 te beperken' (Bijlage 1)
- GGD Gelderland-Midden is toegetreden als Partij (Bijlage 9)
- met betrekking tot het Project: CONTROL: effectiviteit & optimalisatie van bron- en contactonderzoek om de verspreiding van SARS-CoV-2 te beperken;
- Bij deze samenwerking Persoonsgegevens verwerkt zullen worden en tussen Partijen gedeeld;
- Partijen gezamenlijk het doel en de middelen van de verwerking(en) vaststellen en derhalve gezamenlijk verwerkingsverantwoordelijken zijn in de zin van artikel 26 AVG en niet over en weer elkaars Verwerker zijn;
- Partijen, in het kader van een zorgvuldige verwerking van Persoonsgegevens, afspraken wensen te maken over de verwerking van Persoonsgegevens en de wederzijdse verantwoordelijkheden.

zijn als volgt overeengekomen:

Artikel 1. Definities

In deze Overeenkomst hebben de met hoofdletter geschreven begrippen de betekenis zoals deze blijkt uit de Algemene verordening gegevensbescherming. De overige met hoofdletter geschreven begrippen hebben de betekenis zoals in dit artikel opgenomen. Waar de definitie in dit artikel in het enkelvoud is opgenomen, wordt ook het meervoud daaronder begrepen en vice versa, tenzij uitdrukkelijk anders vermeld of uit de context anders blijkt.

- 1.1 Avg: de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de Verwerking van Persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene verordening gegevensbescherming).
- 1.2 Bijlage: een bijlage bij deze Overeenkomst, die een integraal onderdeel vormt van de Overeenkomst.
- 1.3 Bijzondere categorieën Persoonsgegevens: Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid, zoals bedoeld in artikel 9 Avg. Tevens vallen hier strafrechtelijke gegevens in de zin van artikel 10 Avg en het nationaal identificatienummer onder.
- 1.4 Hoofdovereenkomst: de hoofdovereenkomst die tussen Partijen is gesloten in het kader van de Samenwerking en op grond waarvan Partijen Gezamenlijk Verwerkingsverantwoordelijken zijn.

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst

- 1.5 Medewerker: de door Partijen ingeschakelde werknemers en andere personen waarvan de werkzaamheden onder de verantwoordelijkheid van de betreffende Partij vallen en die worden ingeschakeld door die Partij ter uitvoering van de Overeenkomst.
- 1.6 Overeenkomst: de onderhavige overeenkomst inclusief Bijlagen, zoals bedoeld in artikel 26 Avg.
- 1.7 Samenwerking: de samenwerking tussen Partijen op grond van de Hoofdovereenkomst, zoals omschreven in Bijlage 1, waarbij Persoonsgegevens zullen worden uitgewisseld.
- 1.8 Schriftelijk: op schrift gesteld of langs de elektronische weg, zoals bedoeld in artikel 6:227a van het Burgerlijk Wetboek.

Artikel 2. Voorwerp van de Overeenkomst

- 2.1 De Overeenkomst vormt een aanvulling op de Hoofdovereenkomst en vervangt eventuele eerder gemaakte afspraken tussen Partijen ten aanzien van de Verwerking van Persoonsgegevens.
Bij tegenstrijdigheid tussen de bepalingen uit de Overeenkomst en de Hoofdovereenkomst, prevaleren de bepalingen uit de Overeenkomst.
- 2.2 De Overeenkomst is een gezamenlijk-verwerkingsverantwoordelijken overeenkomst waarin Partijen hun respectieve verantwoordelijkheden vastleggen in het kader van de Verwerking (en) van Persoonsgegevens zoals beschreven in Bijlage 2. Partijen zijn gezamenlijke Verwerkingsverantwoordelijken voor de in Bijlage 2 genoemde Verwerking(en).
- 2.3 De bepalingen uit de Overeenkomst gelden voor alle Verwerking(en) die plaatsvinden ter uitvoering van de Samenwerking zoals nader beschreven in de Hoofdovereenkomst. Partijen brengen elkaar onverwijld op de hoogte indien één der Partijen reden heeft om aan te nemen dat hij niet langer aan de Overeenkomst kan voldoen.

Artikel 3. Verplichtingen van Partijen

- 3.1 Partijen verklaren over en weer de Persoonsgegevens op behoorlijke, zorgvuldige en transparante wijze te zullen verwerken, in overeenstemming met Bijlage 2 van deze Overeenkomst en de toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens, in het bijzonder maar niet beperkt tot de Avg en de Telecommunicatiewet.
- 3.2 Partijen zullen de Persoonsgegevens uitsluitend verwerken voor het doeleinde waarvoor de Persoonsgegevens in dit Project zijn verzameld, zoals omschreven in Bijlage 1, tenzij Partijen na voorafgaand overleg Schriftelijk overeenkomen dat Persoonsgegevens tevens mogen worden gebruikt voor doeleinden die daar voldoende nauw mee samenhangen.
- 3.3 Partijen zullen niet meer Persoonsgegevens verzamelen dan strikt noodzakelijk is voor het betreffende doeleinde.
- 3.5 Partijen zullen ieder zelfstandig verantwoordelijk zijn voor het bijhouden van de Verwerking (en) in een passend register van verwerkingsactiviteiten.
- 3.6 De verplichtingen die voortvloeien uit deze Overeenkomst, gelden ook voor degenen die onder het gezag van Partijen Persoonsgegevens verwerken, zoals haar Medewerkers en ingeschakelde Verwerkers.
- 3.7 Partijen dienen op duidelijke en eenvoudige wijze te communiceren waar de Betrokkene voor het uitoefenen van zijn rechten terecht kan, in overeenstemming met de taakverdeling zoals opgenomen in Bijlage 2.

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst

- 3.8 Er wordt als Bijlage 2 een specificatie opgenomen van de Samenwerking tussen Partijen in het kader van de Hoofdovereenkomst en wordt een algemene omschrijving gegeven van deze Samenwerking. Hierin zal tenminste worden opgenomen:
- het doel en een omschrijving van de Samenwerking;
 - de applicatie(s) die bij de samenwerking gebruikt zal/zullen worden;
 - leverancier(s) van de applicatie(s).
- 3.9 In Bijlage 2 is een specificatie opgenomen van de onderlinge verantwoordelijkheden van Partijen en taakverdeling tussen Partijen met betrekking tot zorgvuldige Verwerking van Persoonsgegevens in het kader van de Samenwerking. De volgende aspecten worden in ieder geval in Bijlage 2 vastgelegd:
- welke Partij(en) wanneer verantwoordelijk is (of zijn) voor het sluiten van Verwerkersovereenkomst (en) met Verwerker(s);
 - welke Partij(en) wanneer verantwoordelijk is (of zijn) voor de te treffen technische en organisatorische maatregelen ter beveiliging van Persoonsgegevens in het kader van de Samenwerking;
- 3.10 In Bijlage 2 is een specificatie opgenomen van de Verwerking. De volgende aspecten worden in ieder geval in Bijlage 2 vastgelegd:
- een omschrijving van de Verwerking;
 - de doeleinden van de Verwerking;
 - de categorieën Betrokkenen;
 - de categorieën Persoonsgegevens;
 - de bewaartermijnen;
 - de categorieën Medewerkers die toegang hebben tot de Persoonsgegevens;
 - de Verwerkers die zijn ingeschakeld bij de Verwerking door Partijen;
 - de eventuele doorgiften naar landen buiten de EER;
- 3.11 In Bijlage 2 is een specificatie opgenomen van de door Partijen getroffen technische en organisatorische beveiligingsmaatregelen.
- 3.12 Iedere Partij is zelfstandig verantwoordelijk voor het treffen van passende technische en organisatorische maatregelen ten aanzien van Persoonsgegevens die deze Partij verwerkt in het kader van de Samenwerking.

Artikel 4. Toegang tot Persoonsgegevens

- 4.1 Partijen beperken de toegang tot Persoonsgegevens aan Medewerkers, Verwerkers, Derden en andere Ontvangers van Persoonsgegevens tot een noodzakelijk minimum.
- 4.2 De categorieën Medewerkers die in het kader van de Samenwerking toegang nodig hebben tot Persoonsgegevens, zijn in Bijlage 2 gespecificeerd door Partijen.
- 4.4 Indien een Partij (delen van) de (verdere) Verwerking van de betreffende Persoonsgegevens uitbesteedt aan een Verwerker, draagt hij er zorg voor dat de Verwerker de Persoonsgegevens op behoorlijke en zorgvuldige wijze en in overeenstemming met de toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens verwerkt. Afspraken omtrent de Verwerking van Persoonsgegevens door een Verwerker zullen worden vastgelegd in een passende Verwerkersovereenkomst in de zin van artikel 28 Avg.
- 4.5 Alle Partijen hebben te allen tijde het recht de Verwerkersovereenkomst(en) zoals bedoeld artikel 4.4 in te zien.

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst

- 4.6 Partijen mogen Persoonsgegevens laten verwerken door andere personen of organisaties buiten de Europese Economische Ruimte in overeenstemming met artikel 4.3 t/m 4.5, mits vooraf goedgekeurd door de Partijen en de toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens in acht wordt genomen.

Artikel 5. Geheimhouding en vertrouwelijkheid

- 5.1 Alle Persoonsgegevens worden als vertrouwelijke gegevens gekwalificeerd en dienen als zodanig te worden behandeld. Partijen leggen deze geheimhoudingsplicht tevens op aan alle door Partijen in te schakelen (rechts)personen, waaronder maar niet beperkt tot Medewerkers, Verwerkers, Derden en andere Ontvangers van Persoonsgegevens.
- 5.2 Partijen houden alle Persoonsgegevens geheim en maken deze op geen enkele wijze verder intern of extern bekend, behalve voor zover:
- (i) Bekendmaking en/of verstrekking van de Persoonsgegevens in het kader van de uitvoering van de Hoofdovereenkomst of Overeenkomst noodzakelijk is;
 - (ii) Enig dwingendrechtelijk wettelijk voorschrift of rechterlijke uitspraak van een bevoegde rechtbank of bevel van een andere overheidsinstantie die gezag over Partijen heeft, Partijen tot bekendmaking, verstrekking en/of doorgifte van die Persoonsgegevens verplicht, waarbij Partijen eerst de andere Partijen hiervan op de hoogte stellen, of;
 - (iii) Bekendmaking en/of verstrekking van die Persoonsgegevens geschiedt met voorafgaande Schriftelijke toestemming van de andere Partijen.

Artikel 7. Inbreuk in verband met Persoonsgegevens

- 7.1 De Partij bij wie, of onder wiens verantwoordelijkheid, een Inbreuk in verband met Persoonsgegevens is opgetreden, informeert de overige Partijen binnen 24 uur na constatering van de inbreuk. Partijen zullen in goed overleg bespreken wat de (mogelijke) gevolgen van de Inbreuk zijn voor alle Partijen.
- 7.2 Partijen dragen eigen verantwoordelijkheid om de melding op te nemen in het interne register en/of de Autoriteit Persoonsgegevens in te lichten en verdere afhandeling conform de AVG en Uitvoeringswet AVG.
- 7.3 Partijen zullen elkaar op de hoogte houden van nieuwe ontwikkelingen rondom de inbreuk.
- 7.4 In bijlage 4 is een lijst met contactgegevens van Partijen in geval van een Inbreuk in verband met Persoonsgegevens opgenomen.
- 7.5 Eventuele kosten die gemaakt worden om de inbreuk op te lossen en in de toekomst te kunnen voorkomen, komen voor rekening van de Partij bij wie de inbreuk heeft plaatsgevonden. Partijen kunnen in overleg treden over een eventuele verdeling van deze kosten, indien het gaat om een oplossing die in het belang is van alle Partijen.
- 7.6 Partijen zijn ieder zelf verantwoordelijk voor het bijhouden van een datalekregister.

Artikel 8. Rechten van betrokkenen

- 8.1 In bijlage 2 is opgenomen welke Partij(en) verantwoordelijk is (of zijn) voor het geven van uitvoering aan rechten van Betrokkenen, waaronder de informatieplicht.
- 8.2 Betrokkene die aanspraak wil maken op de uitoefening van zijn recht op inzage, rectificatie, gegevenswissing of gegevensoverdracht, richt zich daartoe tot de Partij die hem als eerste in de verwerking heeft opgenomen.
- 8.3 Partijen hebben de plicht de Betrokkene(n) door te verwijzen naar de Partij die deze als eerste in de verwerking heeft opgenomen.

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst

Artikel 9. Duur en beëindiging

- 9.1 Deze Overeenkomst komt tot stand door ondertekening van Partijen. De duur van de Overeenkomst is gelijk aan de duur van de Hoofdovereenkomst. De Overeenkomst is niet los van de Hoofdovereenkomst te beëindigen. Bij beëindiging van de Hoofdovereenkomst eindigt de Overeenkomst van rechtswege en vice versa.
- 9.2 Partijen mogen deze Overeenkomst alleen wijzigen na overleg met en met toestemming van alle Partijen en zullen zich inspannen om, wanneer wijzigingen in toepasselijke wet- en regelgeving daartoe aanleiding geven, een passende wijziging van deze Overeenkomst te bewerkstelligen.
- 9.3 Iedere Partij is na afloop van de (wettelijke) bewaartermijnen zelf verantwoordelijk voor het vernietigen en/of retourneren van de Persoonsgegevens die zij onder zich heeft en/of die zich bevinden bij een door die Partij ingeschakelde derde, in het kader van deze Overeenkomst. Bewaartermijnen en vernietiging van de data in de onderzoeksomgeving zijn gespecificeerd in Bijlage 2.
- 9.4 Verplichtingen uit de Overeenkomst die naar hun aard bestemd zijn om na beëindiging van de Overeenkomst voort te duren, blijven na beëindiging van de Overeenkomst voortduren.

Artikel 10. Overige bepalingen

- 10.1 De Overeenkomst en de uitvoering daarvan worden beheerst door Nederlands recht.
- 10.2 Alle geschillen, die tussen Partijen mochten ontstaan in verband met de Overeenkomst, zullen worden voorgelegd aan dezelfde rechter die op grond van de Hoofdovereenkomst bevoegd is.
- 10.3 Indien één of meer bepalingen van de Overeenkomst niet rechtsgeldig blijken te zijn, zal de Overeenkomst voor het overige van kracht blijven. Partijen overleggen alsdan over de bepalingen die niet rechtsgeldig zijn, teneinde een vervangende regeling te treffen die wel rechtsgeldig is en zoveel mogelijk aansluit bij de strekking van de te vervangen bepaling.

Bijlagen

- Bijlage 1a Samenwerkingsovereenkomst_Projectvoorstel
- Bijlage 1b Samenwerkingsovereenkomst
- Bijlage 2 Specificatie van de verwerkingen & beveiligingsmaatregelen
- Bijlage 3 Rechten betrokkenen
- Bijlage 4a DPIA GGD Amsterdam
- Bijlage 4b DPIA_BIV GGD Amsterdam
- Bijlage 5 Lijst met variabelen
- Bijlage 6 Contactgegevens Partijen bij Inbreuk ivm Privacy
- Bijlage 7 anDREa GDPR Compliance Assessment
- Bijlage 8 anDREa DPIA
- Bijlage 9 Toetredingsformulier GGD Gelderland-Midden

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst

Aldus overeengekomen en ondertekend,

Partij: GGD Amsterdam

Naam: 5.1.2e 5.1.2e

Functie: 5.1.2e

Datum: 29 juni 2021

Handt

5.1.2e

5.1.2e

29/6/21

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst

Aldus overeengekomen en ondertekend,

Partij: GGD Flevoland

Naam: 5.1.2e

Functie: 5.1.2e

Datum: 07 juli 2021

Handtekening:

5.1.2e

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst

Aldus overeengekomen en ondertekend,

Partij: GGD Gelderland-Midden

Naam:

5.1.2e

Functie:

Datum:

Handtekening:

5.1.2e

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst

Aldus overeengekomen en ondertekend,

Partij: GGD Groningen

Naam: 5.1.2e 5.1.2e

Functie: 5.1.2e

Datum: 05-07-2021

Handtekening:

5.1.2e

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst

Aldus overeengekomen en ondertekend,

Partij: GGD Hart voor Brabant

Naam:

Functie:

5.1.2e

Datum:

5 juli 2021

Handtekening:

5.1.2e

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst

Aldus overeengekomen en ondertekend,

Partij: GGD Regio Utrecht

Naam:

Functie:

5.1.2e

Datum:

17-7-2021

Handtekening:

5.1.2e

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst

Aldus overeengekomen en ondertekend,

Partij: GGD Rotterdam-Rijnmond

Naam:

Functie:

5.1.2e

Datum: 9 juli 2021

Handtekening

5.1.2e

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst

Aldus overeengekomen en ondertekend,

Partij: GGD Zuid-Limburg

Naam:

Functie:

5.1.2e

Datum: 05-07-2021

Handtekening:

5.1.2e

Bijlage 1a & 1b

Samenwerkingsovereenkomst met als bijlage het Projectvoorstel

16 - 70

Dubbel

Bijlage 2. Specificatie van de Verwerking & Beveiligingsmaatregelen

Inhoudsopgave

Inhoudsopgave	1
Definities.....	2
Omschrijving van de Verwerking en Verantwoordelijkheden	3
Doeleinden van de Verwerking.....	5
Categorieën Betrokkenen	6
Informeren Betrokkenen	6
Uitoefening recht op inzage, rectificatie of gegevenswissing van Betrokkenen	6
Bewaartermijnen & archivering.....	6
Categorieën Medewerkers die toegang hebben tot de Persoonsgegevens;.....	7
Categorieën Persoonsgegevens	7
Specificatie getroffen technische en organisatorische beveiligingsmaatregelen	7
Genereren data bestanden voor het Project	7
Data upload, opslag en analyse	8
Technische beveiligingsmaatregelen.....	8
Organisatorische beveiligingsmaatregelen	9
Delen van data met externe partijen en onderzoekers anders dan de samenwerkingspartners	9

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst, Bijlage 2

Definities

Bron systeem	Database systeem waarin ruwe data zijn opgeslagen die zijn verzameld in de corona test- en BCO-keten routines. Dit zijn CoronIT, HPZone en Osiris data.
Data manager	Persoon werkzaam bij een Partij die de bevoegdheid heeft te werken met de routinematig verzamelde data uit de corona test- en BCO-keten, deze data te extraheren, op te slaan en uit te geven in het kader van dit Project en lid is van de Werkgroep van het Project.
Data steward	Persoon werkzaam bij de GGD Amsterdam die Admin rechten heeft in de Cloud omgeving en het data management uitvoert op de gezamenlijke data van de Partijen, zorg draagt voor de opslag, archivering en verwijdering van de Onderzoeksdata.
Gebruiker	Een persoon werkzaam bij een Partij die gespecificeerde toegang heeft tot de Onderzoeksomgeving
Hoofdovereenkomst	Samenwerkingsovereenkomst met bijlagen die Partijen gezamenlijk hebben ondertekend
Onderzoeker	Gebruiker van de Onderzoeksomgeving aan wie door de Stuurgroep rechten zijn toegekend om onderzoeksdata te analyseren;
Onderzoeksomgeving	Digital Research Cloud (DRE), het cloud platform voor het Project
Overeenkomst	De onderhavige gezamenlijke verwerkersovereenkomst;
PI	Principal Investigator die binnen de Partij verantwoordelijkheid draagt voor het Project;
Project	Het planmatige geheel aan activiteiten zoals omschreven in de Aanvraag – opgenomen als Bijlage 1 van de Hoofdovereenkomst
Projectleider	Toezietherouder op het verloop van het Project of deelaspecten daarvan;
Projectvoorstel	De uitgewerkte projectaanvraag zoals gehonoreerd door ZonMW
Resultaten	Alle uitkomsten, materialen, methodes, processen, producten, software, (uit)vindingen, of data die binnen een Project worden gegenereerd. Deze zijn anoniem;
Stuurgroep	Principal Investigators van Partijen en de Projectleider die gezamenlijk de verantwoordelijkheid dragen voor de voortgang van het Project

Omschrijving van de Verwerking en Verantwoordelijkheden

Ten behoeve van het Project worden routinematig verzamelde Persoonsgegevens in de corona test- en bron- en contactonderzoek keten verwerkt.

In voorbereiding op het uitwisselen van data vinden er enkele verwerkingen plaats bij de Partijen:

- 1) De Data manager van de Partij extraheert data, waaronder Bijzondere Persoonsgegevens en Persoonsgegevens, uit de Bron systemen en vraagt OSIRIS data van de GGD regio op bij het Rijksinstituut voor Volksgezondheid en Milieu (RIVM).
- 2) De Data manager voegt de bestanden samen en archiveert dit bestand conform bewaartermijnen benoemd in de sectie 'Bewaartermijnen & archivering' en lokale archiveringsstandaard.
- 3) De Data manager voert data bewerkingen uit op de geëxtraheerde data, waaronder het koppelen van de data uit de Bron systemen. Voor deze koppeling worden direct herleidbare Persoonsgegevens gebruikt.
- 4) Na deze koppeling verwijdert de Data manager uit de onderzoeksdataset direct herleidbare Persoonsgegevens, namelijk achternaam en eventueel nog andere aanwezige direct herleidbare gegevens zoals e-mailadres, verzekeringsnummer of telefoonnummer. Identificatienummers worden verwijderd en vervangen door niet herleidbare studienummers.
- 5) (Bijzondere) Persoonsgegevens die nodig zijn voor het uitvoeren van het Project blijven in de het databestand behouden.

De verwerkingen 1 tot en met 5 gebeuren door de data eigenaren – de Partijen. Zij zijn verantwoordelijk voor het uitvoeren van deze stappen. Ter ondersteuning verstrekt CONTROL een handleiding en een R script die deze stappen uitvoert.

Binnen het Project vinden de volgende Verwerkingen plaats:

- 6) De Data manager van de Partij uploadt het verkregen databestand naar de Onderzoeksomgeving. De Partij dient ervoor te zorgen dat het uploaden gebeurt vanuit een voldoende beveiligde werkomgeving.
- 7) De Data steward importeert deze gepseudonimiseerde data in de MySQL database in de Onderzoeksomgeving.
- 8) In de Onderzoeksomgeving voert de Data steward databewerkingen uit op de geüploade data t.b.v. data harmonisatie
- 9) Geüploade bestanden worden binnen 30 dagen na uploaden in de Onderzoeksomgeving verwijderd. Hiervan ontvangt de Data manager een bevestiging per email.
- 10) De Onderzoeker logt in op de Onderzoeksomgeving en voert analyses uit met de applicaties die beschikbaar zijn in de Onderzoeksomgeving, conform het Projectvoorstel of conform aanvullende afspraken gemaakt door de Stuurgroep en vastgelegd in een onderzoeksvoorstel, zoals omschreven in de Hoofdovereenkomst, opgenomen als Bijlage 1 van de Overeenkomst.
- 11) Gegenereerde Resultaten worden opgeslagen in de Onderzoeksomgeving, kopieën van deze Resultaten worden gedownload door de Onderzoeker naar de lokale werkomgeving en gebruikt in de wetenschappelijke output van het Project. Deze Resultaten bevatten geen Persoonsgegevens.

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst, Bijlage 2

- 12) Publieke openbaarmaking van Resultaten door middel van wetenschappelijke publicatie of anderszins wordt vooraf ter goedkeuring voorgelegd aan de Stuurgroep, zoals omschreven in de Hoofdovereenkomst, opgenomen als Bijlage 1 van de Overeenkomst.

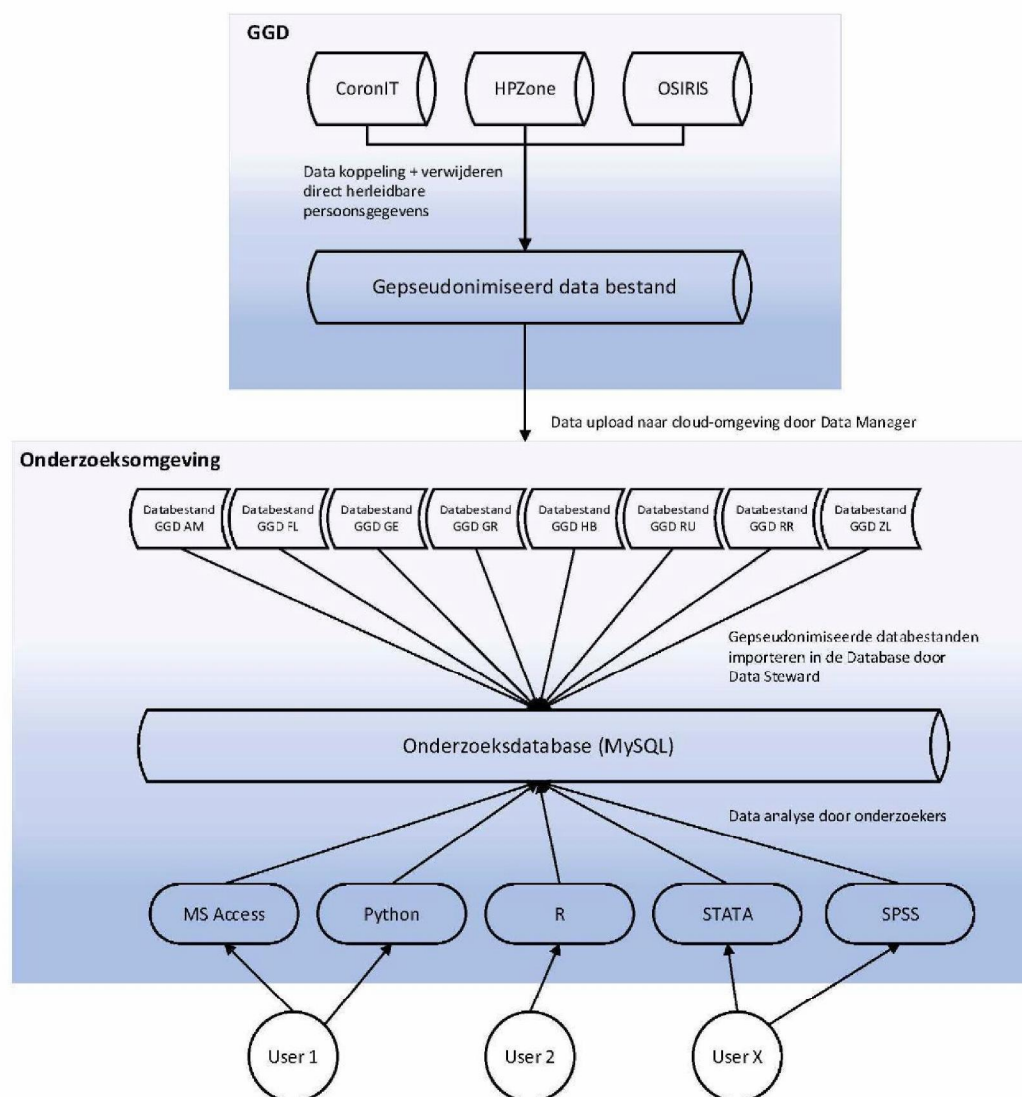
De GGD Amsterdam is verantwoordelijk voor de verwerkingen die plaatsvinden in de Onderzoeksomgeving en sluit hiervoor passende overeenkomsten af met de Verwerker en de Gebruikers van de Onderzoeksomgeving.

De Partij die verantwoordelijk is voor de Verwerking dient passende organisatorische en technische maatregelen te treffen ter bescherming van de Data.

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst, Bijlage 2

Het *Figuur* geeft een schematische weergave van de verwerkingen in het CONTROL project.

Figuur: Schematische weergave van de Verwerking van Data, Persoonsgegevens en Bijzondere Persoonsgegevens binnen het Project en in de context waarin deze plaatsvinden.



Doeleinden van de Verwerking

De Verwerkingen worden uitgevoerd ten behoeve van het Project vastgelegd in de Hoofdovereenkomst (bijlage 1 van de Overeenkomst). In het kort: het doel van de verwerkingen is om Data van de Partijen bij elkaar te brengen en deze Data te analyseren ter beantwoording van de onderzoeksvragen omschreven in het Projectvoorstel of aanverwante onderzoeksvragen na besluit van de Stuurgroep. Het onderzoek omvat een procesevaluatie naar de effectiviteit van het bron- en contactonderzoek in de corona testketen

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst, Bijlage 2

met het doel factoren te identificeren die de effectiviteit beïnvloeden en triageringstools te ontwikkelen ter optimalisatie van deze processen. Het betreft wetenschappelijk operationeel onderzoek met een groot belang voor de Infectieziekten bestrijding. De grondslag voor dit onderzoek is art. 6.1.e, art. 9.j en art. 89.1 en uavg art 24. Onder de Wgbo is de grondslag voor deze studie art 7:458.

Categorieën Betrokkenen

De Betrokkenen zijn personen woonachtig in de GGD regio's Amsterdam, Flevoland, Gelderland Midden, Groningen, Hart voor Brabant, Regio Utrecht, Rotterdam-Rijnmond en Zuid Limburg en die op enigerlei wijze voorkomen in de Bron systemen. In de periode van 1 juni 2020 t/m 28 februari 2021 zijn er meer dan 5 miljoen coronatesten uitgevoerd. Aangezien Betrokkenen zich vaker dan één keer kunnen laten testen is het aantal Betrokkenen lager dan het aantal uitgevoerde testen.

Informereren Betrokkenen

De Partij(en) die verantwoordelijk is (zijn) voor de Verwerking heeft (hebben) een informatieplicht naar de Betrokkene(n). Partijen verlenen inzage en verstrekken informatie aan elkaar en de Betrokkene(n) als hierom wordt gevraagd. Partijen dienen op duidelijke en eenvoudige wijze te communiceren waar de Betrokkene terecht kan voor het uitoefenen van rechten met betrekking tot de verwerking van (Bijzondere) Persoonsgegevens, waaronder het recht op inzage, wijziging en verwijdering van deze gegevens.

Partijen informeren Betrokkene(n) in een privacyverklaring over de wijze en grondslag van verwerking van (Bijzondere) Persoonsgegevens en het recht op inzage, wijziging en verwijdering van deze gegevens. De privacy verklaringen worden gepubliceerd op de lokale GGD websites.

Uitoefening recht op inzage, rectificatie of gegevenswissing van Betrokkenen

Betrokkene(n) hebben het recht te weten welke persoonsgegevens worden verwerkt in het CONTROL project, deze te wijzigen en te laten verwijderen. Het document 'Werkinstructie – Rechten Betrokkene(n) t.a.v. inzage, rectificatie en verwijdering' beschrijft hoe deze rechten zijn gewaarborgd in CONTROL. De werkinstructie is opgenomen als Bijlage 3 van de Gezamenlijke Verwerkersverantwoordelijken overeenkomst.

Bewaartermijnen & archivering

Binnen 2 maanden na beëindigen van het Project, conform de Hoofdovereenkomst (Bijlage 1), worden (Bijzondere) Persoonsgegevens en overige data die niet zijn gebruikt in de Resultaten van het Project vernietigd. De projectleider bevestigt de vernietiging van deze gegevens in een email aan de Data manager van de Partij en stuurt met deze bevestiging een samenvatting van de vernietigde gegevens.

Voor (Bijzondere) Persoonsgegevens en overige data die zijn gebruikt bij het genereren van een Resultaat van het Project wordt een bewaartermijn van vijf jaar gehanteerd na wetenschappelijke publicatie. Deze Data worden gearchiveerd op de lokale beveiligde server van de GGD Amsterdam. Toegang tot de gearchiveerde bestanden hebben de Projectleider en de Data steward. Na de bewaartermijn worden de

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst, Bijlage 2

gegevens vernietigd. De Projectleider bevestigt de vernietiging van deze gegevens in een email aan de PI van de Partij en stuurt met deze bevestiging een samenvatting van de vernietigde gegevens.

Categorieën Medewerkers die toegang hebben tot de Persoonsgegevens;

In de Onderzoeksomgeving wordt er onderscheid gemaakt tussen de volgende taken en rechten:

- A) Importeren en inzien van data van een Partij
- B) Wijzigen en verwijderen van Data van alle Partijen
- C) Inzien en analyseren van Data van alle Partijen
- D) Beheer van toegangsrechten

Toegang tot de (Bijzondere) Persoonsgegevens en overige data van Partijen en taken/rechten hebben de volgende categorieën medewerkers:

- Data manager van een Partij: A
- Onderzoeker: C
- Data steward: A, B, C, D
- Projectleider: A, B, C, D

Categorieën Persoonsgegevens

In Bijlage 5 is een lijst opgenomen met variabelen, het bronsysteem waaruit de variabele afkomstig is, de categorie Persoonsgegevens waartoe de variabele behoort en het doel/reden van het gebruik in het project.

Samenvattend worden de volgende categorieën Bijzondere Persoonsgegevens verwerkt:

- Geboorteland
- Gegevens waaruit religieuze of levensbeschouwelijke overtuigingen blijken
- Gegevens over gezondheid

Samenvattend worden de volgende categorieën Persoonsgegevens verwerkt:

- Gegevens waaruit woonlocatie afgeleid kan worden
- Gegevens die informatie geven over de identiteit en de persoonlijke levenssfeer van de Betrokkene(n)

Specificatie getroffen technische en organisatorische beveiligingsmaatregelen

Genereren data bestanden voor het Project

Ter voorbereiding op het leveren van data voor het Project worden Persoonsgegevens, Bijzondere Persoonsgegevens en overige data die zijn opgeslagen in de Bron systemen door de Data manager van de Partij geëxtraheerd conform eigen procedures en opgevraagd bij het RIVM. De verkregen data bestanden worden door de Partijen zelf lokaal aan elkaar gelinkt. Direct na linken worden direct herleidbare

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst, Bijlage 2

Persoonsgegevens verwijderd. Als identifier in het bestand wordt een gepseudonimiseerde identifier toegekend aan de records. De Data steward verstrekt een R script waarmee de data koppeling en pseudonimisatie stap kunnen worden uitgevoerd. Het script verwijderd tevens direct herleidbare Persoonsgegevens. Dit waarborgt het goed uitvoeren van de pseudonimisatie stap met behoud van kwaliteit en uniformiteit van de data tussen Partijen. Data in het resulterende onderzoeksbestand van de Partij zijn gepseudonimiseerd en gecodeerd en niet direct te herleiden naar de Betrokkenen.

Data upload, opslag en analyse

Partijen maken voor de transfer, opslag en analyse gebruik van anDREa, een cloud-based workspace (de Onderzoeksomgeving). GGD Amsterdam sluit een Verwerkersovereenkomst af met anDREa. Alle resources en virtuele machines werken in een Microsoft Azure Data Center gestationeerd in de EU/EEA (Amsterdam). De Onderzoeksomgeving is compliant met AVG en ISO/IEC/27001:2013 en heeft een CIA/BIV classificatie. Gedetailleerde omschrijvingen van geïdentificeerde beveiligingsrisico's en getroffen beveiligingsmaatregelen met betrekking tot de Onderzoeksomgeving, evenals compliance assessments met de AVG, ISO/IEC/27001:2013 en CIA/BIV classificatie zijn te vinden op <https://andrea.helpmydre.org/home>. De [GDPR Compliance Assessment \(versie vo.8, augustus 2020\)](#) en de [DPIA \(versie v1.0, augustus 2020\)](#) zijn toegevoegd als Bijlage 7 en 8 van de Overeenkomst.

Data analyse vindt plaats binnen de Onderzoeksomgeving met de volgende software of nieuwere versies wanneer deze beschikbaar komen

R 4.0.2	MS Office 2016
Python 3.8.2	SPSS 25
Power BI 2.70.5494.761	
Ook kunnen geïnstalleerd worden:	STATA Intercooled 16 en SAS

Technische beveiligingsmaatregelen

- 1) Data zijn gepseudonimiseerd en privacy gevoelige gegevens zijn gecodeerd (zie specificatie in Bijlage 5).
- 2) Data worden vanaf de lokale GGD'en direct geüpload in de onderzoeksomgeving.
- 3) Data transfer en data opslag zijn encrypted.
- 4) Downloaden van data uit de Onderzoeksomgeving is geblokkeerd en kan alleen na expliciete toestemming van de Projectleider en Data steward.
- 5) Toegangsrechten tot de Onderzoeksomgeving worden uitgegeven, gemonitord en gewijzigd door de Projectleider (tevens huurder van de omgeving) en Data steward in overeenstemming met de Stuurgroep.
- 6) Toegangsrechten worden aangevraagd bij de Projectleider door middel van het invullen van de Gebruikersovereenkomst (Gebruikersvoorwaarden_Onderzoeksomgeving_vs1.doc).
- 7) De Projectleider meldt de nieuwe gebruiker met de naam, het emailadres en het telefoonnummer aan bij de DRE, waarna het account wordt aangemaakt. Zie https://docs.google.com/document/d/1Q-1FEVhtJlncYO7BX-CFlzX_QCA_RdyMz6of8SwnXI/edit# voor de procedure van het aanmaken van een account. Het account wordt geactiveerd door middel van een twee-factor-authenticatie (2FA).
- 8) Er is 2FA voor toegang tot de workspace.
- 9) Toegang en pogingen door niet-geautoriseerde personen om toegang te krijgen worden gelogd.
- 10) Geüpload data kunnen niet zonder expliciete toestemming van de Projectleider of Data steward worden gedownload of verwijderd. In de Onderzoeksomgeving kan een verzoek tot downloaden

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst, Bijlage 2

of verwijderen worden gedaan en deze wordt geautomatiseerd per email verstuurd aan de Projectleider en de Data steward die dit verzoek vervolgens kunnen honoreren.

- 11) Geüploade data worden in de Onderzoeksomgeving geanalyseerd met behulp van programma's die binnen deze omgeving zijn geïnstalleerd en worden geüpdatet.
- 12) De inrichting van de Onderzoeksomgeving, inclusief het installeren en updaten van software is voorbehouden aan de Data steward en de Projectleider die Admin rechten hebben in de Onderzoeksomgeving.

Organisatorische beveiligingsmaatregelen

- 1) De Projectleider is verantwoordelijk voor het aanvragen, bijhouden en intrekken van toegangsrechten van gebruikers van de Onderzoeksomgeving en monitort de inloggeschiedenis van de Onderzoeksomgeving. De Stuurgroep wordt hiervan tenminste eens per kwartaal tijdens het stuurgroep overleg op de hoogte gehouden en tussentijds wanneer is geconstateerd dat er oneigenlijke inlogpogingen of poging tot het downloaden/verwijderen van data zijn gedaan.
- 2) Admin rechten zijn belegd bij de Projectleider en de Data steward.
- 3) Een gebruiker van de Onderzoeksomgeving dient akkoord te gaan met de gebruikersvoorwaarden van anDREa en met de aanvullende gebruikersvoorwaarden van de Onderzoeksomgeving van het Project.
- 4) In de Onderzoeksomgeving worden geüploade databestanden bewerkt en opgeslagen in de MySQL database. De geüploade bestanden worden binnen 30 dagen na uploaden vernietigd. Hiervan wordt de Data manager van Partij per e-mail op de hoogte gebracht.
- 5) Na beëindiging/afronding van het Project worden de data in de omgeving vernietigd en de Onderzoeksomgeving opgeheven in opdracht van de Projectleider, tevens huurder van de Onderzoeksomgeving. Dertig dagen na verwijderen wordt ook de back-up verwijderd en is de data vernietigd. Deze vernietigingen worden gelogd. De PI's van Partijen worden per e-mail op de hoogte gebracht van de vernietiging.

Delen van data met externe partijen en onderzoekers anders dan de samenwerkingspartners

Voor de vindbaarheid wordt de data verzameling aangemeld bij een online repository en worden de Meta data openbaar gemaakt via deze repository. Externe onderzoekers kunnen een verzoek tot gebruik van de Data samen met een onderzoeksvoorstel indienen bij de Stuurgroep. De aanvraag wordt door de Stuurgroep beoordeeld op kwaliteit, overlap met eigen onderzoeksplannen en wetgeving, waarna een beslissing volgt over het al dan niet delen van data met de externe partij. De Partijen dragen ieder voor zich zorg voor het volgen van interne procedures ten aanzien van het delen van data, zoals bijvoorbeeld het consulteren van een jurist alvorens toestemming te geven.

De volgende uitgangspunten worden gehanteerd bij de uitgifte van Data aan externe onderzoekers:

- 1) De dataset is tenminste gepseudonimiseerd;
- 2) Van elke variabele in de dataset is aannemelijk gemaakt dat deze nodig is voor het voorgestelde onderzoek;

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst, Bijlage 2

- 3) De data uitwisseling wordt vastgelegd in een passende overeenkomst die wordt ondertekend door de Partijen waarvan data wordt geleverd en de aanvrager alvorens Data worden gedeeld. In deze overeenkomst wordt tenminste opgenomen:
- a. Doel van de verwerking;
 - b. Gebruik- en bewaartermijnen;
 - c. Beveiliging;
 - d. Eigenaarschap;
 - e. Lijst met variabelen en de grondslag voor verwerking.

Data uitwisseling met externe partijen buiten de EER is slechts mogelijk wanneer alle Partijen daarmee hebben ingestemd. Elk verzoek tot data uitwisseling van een niet-EER land wordt gezamenlijk besproken en over beslist. In alle gevallen wordt de bescherming van Persoonsgegevens gewaarborgd in een passende overeenkomst waarin tenminste zijn opgenomen:

- a. Doel van de verwerking;
- b. Gebruik- en bewaartermijnen;
- c. Beveiliging;
- d. Eigenaarschap;
- e. Lijst met variabelen en de grondslag voor verwerking;
- f. Bepalingen opgenomen in artikel 46(2) van de AVG.

Rechten Betrokkene(n) t.a.v. inzage, rectificatie en verwijdering

Datum: 8 juni 2021

Betrokkene(n) hebben het recht te weten welke persoonsgegevens worden verwerkt in het CONTROL project, deze te wijzigen en te laten verwijderen. Dit document beschrijft hoe deze rechten zijn gewaarborgd in CONTROL.

De data waarmee CONTROL werkt zijn gepseudonimiseerd. CONTROL heeft geen direct herleidbare gegevens. Variabelen waarmee iemand direct te herleiden is worden door de GGD'en lokaal verwijderd voordat de data aan CONTROL worden verstrekt.

Waar kan een Betrokkene zich melden?

Wanneer een Betrokkene gebruik wil maken van het recht op inzage, wijziging of verwijdering dient de betrokkene zich te melden bij de GGD die de persoon als eerste in de verwerking heeft opgenomen (1^{ste} GGD). Dit is beschreven in de Gezamenlijke verwerkersverantwoordelijken overeenkomst. De 1^{ste} GGD is de GGD in de regio waar de persoon woonde op het moment dat deze werd ingeschreven in CoronIT en/of HPZone. Directe aanmelding bij GGD Amsterdam/CONTROL kan niet, want GGD Amsterdam kan cliënten van andere GGD'en niet verifiëren. Als een persoon zich bij een andere GGD uit het CONTROL project aanmeldt wordt de persoon doorverwezen naar de 1^{ste} GGD. De doorgeefplicht is ook opgenomen in de Gezamenlijke verwerkersverantwoordelijken. Tenminste op de CONTROL website van de GGD Amsterdam zal dit kenbaar gemaakt worden.

Verificatie

De gegevens van een persoon mogen alleen worden ingezien, gewijzigd of verwijderd wanneer is geverifieerd dat het om de juiste persoon gaat. De GGD'en hebben hier een eigen werkwijze voor die zal worden gevolgd. De geverifieerde link tussen de persoon en de CONTROL data kan worden gelegd in het archief/bron bestand.

Inzage

De 1^{ste} GGD stemt af met de Betrokkene waarin deze persoon inzage wil. De 1^{ste} GGD kan desgevraagd op individueel niveau inzage geven in de gegevens die uit de bronsystemen zijn geëxtraheerd vanuit het archief bestand dat lokaal is opgeslagen. Dit is het enige bestand waarin voldoende persoonsgegevens staan om met zekerheid te kunnen zeggen dat het om de Betrokkene in kwestie gaat. Lokaal kan er ook inzage gegeven worden in de databewerkingen die worden uitgevoerd en de gegevens die naar de onderzoeksomgeving van CONTROL worden geëxporteerd.

Wanneer de Betrokkene inzage wil in de verwerkingen die in de onderzoeksomgeving gedaan zijn met de gegevens van Betrokkene kan de Data manager of Principal investigator van de 1^{ste} GGD het verzoek mailen naar 5.1.5@ggd.amsterdam.nl. In het verzoek dienen enkele kenmerken (veel gebruikte in- en exclusie criteria in studies) van de persoon te staan waarmee achterhaald kan worden in welke analyse de persoon is opgenomen. Kenmerken zijn bijvoorbeeld woonplaats, testdatum, geslacht, leeftijd. De GGD Amsterdam rapporteert aan de 1^{ste} GGD in welke analyses/rapportages/artikelen, etc. gegevens van de persoon zijn opgenomen.

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst, Bijlage 3
Werkinstructie – Rechten Betrokkene(n) t.a.v. inzage, rectificatie en verwijdering

Rectificatie & verwijdering

De 1^{ste} GGD stemt af met de Betrokkene welke gegevens gerectificeerd of verwijderd dienen te worden. De 1^{ste} GGD is verantwoordelijk voor aanpassingen in lokaal opgeslagen of gearchiveerde CONTROL databestanden en volgt lokale beveiligingseisen. GGD Amsterdam is verantwoordelijk voor het doorvoeren van wijzigingen/verwijderingen zoals aangeven door de 1^{ste} GGD in het databestand in de onderzoeksomgeving.

De rectificatie/verwijdering kan op de volgende manieren worden doorgevoerd in de onderzoeksomgeving:

- 1) De 1^{ste} GGD gaat voor het individu wiens data gerectificeerd of verwijderd moet worden in het bronbestand na wat diens hash-id is. Dit is een uniek identificatienummer wat aangemaakt wordt door een algoritme, wat niet te herleiden is tot bestaande identificatienummers, waarmee de informatie van deze persoon in het databestand kan worden teruggevonden. Dit hash-id wordt doorgegeven aan de Data steward van CONTROL door een e-mail te sturen naar 5.1.5 @ggd.amsterdam.nl. De Data steward voert de rectificatie of verwijdering uit.
- 2) De 1^{ste} GGD stelt een lijst met gegevens op waarmee het individu geïdentificeerd kan worden. De lijst bevat voldoende kenmerken zodat slechts 1 persoon in het databestand aan die unieke combinatie van kenmerken voldoet (een combinatie van leeftijd, testdatum, geslacht en andere variabelen). De lijst met gegevens wordt doorgegeven aan de Data steward van CONTROL door een e-mail te sturen naar 5.1.5 @ggd.amsterdam.nl. De Data steward voert de rectificatie of verwijdering uit.
- 3) De Data manager van de 1^{ste} GGD voert lokaal de rectificatie/verwijdering door in de databestanden en uploadt een nieuw databestand in de onderzoeksomgeving. De Data steward vervangt het oude bestand voor het nieuwe.

Afhandeling/archivering verzoeken

De Data steward meldt per e-mail aan de 1^{ste} GGD dat het verzoek is verwerkt. Deze email wordt door CONTROL gearchiveerd.

Bijlage 4a

DPIA Amsterdam

Gemeente Amsterdam - Data Protection Impact Assessment (DPIA)



Cluster: Sociaal
Directie: GGD
Procesnaam (bedrijfsproces):
Datum: 13-04-2021 (datum laatste versie: 25 juni 2021)

Opdrachtgever: ZonMw

Versie: 5.0

Auteur:

Functie: 5.1.2e

Vraag		Beantwoordingsveld
Deel 1 - Algemeen		
1	Is dit een nieuw proces, of een nieuwe versie van een bestaand proces?	Ja, het betreft nieuw wetenschappelijk operationeel onderzoek waarbij datastromen van meerdere GGD'en bij elkaar worden gebracht in een cloud-based Onderzoeksomgeving ten behoeve van een
2	Is er een DPIA gedaan voor eerdere versies van dit proces?	Nee
3	Is iets veranderd sinds de laatste DPIA is uitgevoerd?	Nvt
4	Beschrijf het proces en de (voorgenomen) verwerkingsactiviteiten en/of het voorgenomen beleid/regelgeving waarvoor deze DPIA wordt uitgevoerd.	Door de GGD Amsterdam, GGD Flevoland, GGD Groningen, GGD Gelderland-Midden, GGD Hart voor Brabant, GGD Rotterdam-Rijnmond, GGD Utrecht en GGD Zuid-Limburg wordt binnen het corona test beleid in de reguliers praktijk data verzameld (coronIT data, HP2one data en OSIRIS data). Deze data worden door de GGD'en gepseudoniseerd geüpload in de cloud based Onderzoeksomgeving. Data analyse gebeurt ook in de beschijfde cloud-based workspace met een virtueel machine. Geanonimiseerde rapportages worden gepubliceerd.
5	Beschrijf eventuele (nieuwe) technologieën voor zover daarvan gebruik wordt gemaakt bij dit proces? Bijvoorbeeld internet of things, wifi tracking of behavioral advertising.	De data worden opgeslagen in een cloud-based Onderzoeksomgeving, anDREA. Deze Omgeving bestaat al en is niet nieuw in het kader van dit project opgezet. Daarnaast wordt cloud opslag, en het gebruik van virtueel machines al jarenlang toegepast.
6	Betreft deze DPIA een enkele verwerking, of een reeks verwerkingen met een vergelijkbaar risico?	Er wordt eenmalig data geüpload en geüpload in Onderzoeksomgeving door de Partijen. Deze zullen meermalen gebruikt worden voor statistische analyses.
7	Wat zijn de doelen van de verwerkingen van persoonsgegevens binnen het proces?	Het doel van de verwerkingen is wetenschappelijk operationeel onderzoek uitvoeren. Het doen van een procesevaluatie en vergelijkend onderzoek, naar de keten van testen, bron- en contactonderzoek, en quarantaine voor SARS-CoV-2, uitgevoerd door GGD'en die participeren in dit tweejarige project. (zie bijlage 1. CONTROL Consortiumovereenkomst)
8	Beschrijf de (categorieën van) betrokkenen waarvan persoonsgegevens worden verwerkt. Benoem of er sprake is van kwetsbare groepen.	Gegevens worden verwerkt van alle personen in de 8 genoemde GGD regio's die zich aanmelden voor een coronatest of op een andere wijze zijn getest waarvan de uitslag is doorgegeven aan de GGD'en. Personen die tot kwetsbare groepen behoren (kinderen, ouderen, etc) kunnen onderdeel zijn van deze data.
9	Geef aan welke (categorieën van) persoonsgegevens worden verwerkt?	Gezondheid, leeftijd, geboorteland, beroep, contacten en bezochte locaties, waardoor een algemeen beeld kan worden verkregen van de levenssfeer van de individu.
10	Worden er ook bijzondere persoonsgegevens, strafrechtelijke persoonsgegevens en/of BSN verwerkt? Zo ja, geef aan welke gegevens.	Ja, van individuen met een positieve testuitslag wordt geboorteland verkregen en locaties die zijn bezocht in de infectieus periode. De informatie over de bezochte locaties kan het mogelijk maken om inzicht te krijgen over de religieuze of levensbeschouwelijke overtuigingen wanneer die bezochte locatie een religieus gebouw betreft. CONTROL gebruikt niet actief informatie over religie of levensbeschouwing, maar kan dit door de locatie gegevens mogelijk wel afleiden.
11	Geef aan op welke gegevensdrager de persoonsgegevens worden opgeslagen (hardware, software, netwerken).	De data worden geüpload van de afgeschermden systemen van de GGD'en zelf naar de Cloud-based Digital Research Environment (ontwikkeld door Radboud MC), Microsoft Azure Data Center geüpload in de EU/EEA (Amsterdam).
12	Zijn de bewaartermijnen in kaart gebracht? Zo ja, geef aan wat de bewaartermijnen zijn.	Er wordt voor dit project geen additionele dataverzameling uitgevoerd, alle data die worden gebruikt in het project worden in het project worden in het corona testkaten. De ruwe data zijn opgeslagen in coronIT en HP2one met de GGD'en als data eigenaren. Deze ruwe bron data zijn niet van CONTROL. CONTROL gebruikt kopieën van de originele data. CONTROL hanteert bewaartermijnen van 5 jaar voor data die uiteindelijk zijn gebruikt in rapportages en wetenschappelijke publicaties. Data die niet zijn gebruikt in de publicaties worden direct na beëindiging van het project verwijderd. Dit is vastgelegd in de gezamenlijke verwerkersovereenkomst.
13	Van hoeveel individuen worden er (ongeveer) persoonsgegevens verwerkt in het kader van dit proces?	betrokkenen zijn personen woonachtig in de GGD regio's Amsterdam, Flevoland, Gelderland-Midden, Groningen, Hart voor Brabant, Rotterdam-Rijnmond, Regio Utrecht en Zuid Limburg, die op enigerlei wijze voorkomen in de Bron systemen. In de periode van 1 juni 2020 t/m 31 oktober 2020 zijn er ~1,5 miljoen coronatesten afgenomen en dit aantal groeit met ongeveer 100.000 tot 150.000 per week. Aangestreefde betrokkenen zich vaker dan één keer kunnen laten testen is het aantal betrokkenen lager dan het aantal uitgevoerde testen.
Deel 2 - Betrokken actoren		
14	Zijn alle partijen die in contact komen met de persoonsgegevens in kaart gebracht?	Ja, deze zijn geïdentificeerd in bijlage 2 van de gezamenlijke verwerkersverantwoordelijke overeenkomst. Dit zijn: de verstrekkers van de data bij de GGD'en (data managers genoemd). Bij GGD Amsterdam betreft het 5.1.2e en 5.1.2e en de onderzoekers op het project. Medewerkers van de onderzoeksomgeving hebben geen toegang tot de non-encrypted data.
15	Welke interne en externe verantwoordelijken zijn betrokken bij dit proces?	College van B&W
16	Zijn er afspraken gemaakt met andere verantwoordelijken over de verwerking van persoonsgegevens?	De data uitwisseling en verwerkingen die in het kader van dit project plaatsvinden bij de GGD'en en de verantwoordelijken zijn vastgelegd in een gezamenlijke verwerkersverantwoordelijke overeenkomst.
17	Zijn er verwerkers betrokken bij het proces? Zo ja, noem de verwerkers.	Ja, Verwerkingsverantwoordelijken zijn GGD Amsterdam, GGD Flevoland, GGD Gelderland-Midden, GGD Groningen, GGD Hart voor Brabant, GGD Rotterdam-Rijnmond, GGD Regio Utrecht, GGD Zuid Limburg. Verwerker is anDREA

18	Is er een verwerkersovereenkomst afgesloten met de verwerkers?	Er wordt een gezamenlijke verwerkersverantwoordelijke overeenkomst opgesteld tussen de samenwerkende GGD'en. Deze DPIA is bijlage in deze overeenkomst. Ondertekening gebeurt als alle Partijen akkoord zijn met de documenten. Daarnaast wordt er een verwerkersovereenkomst opgesteld tussen GGD Amsterdam en anDREa, de verstrekker van de Digital Research Environment. Ook dit proces loopt parallel aan het opstellen van deze DPIA.
19	Zijn er ontvangers betrokken bij dit proces? Zo ja, is er een overeenkomst met de ontvanger?	Nee
20	Worden persoonsgegevens doorgegeven naar landen buiten de Europese Unie? Zo ja, geef aan om welke partijen het gaat en welke waarborgen hiervoor zijn genomen.	Nee. Er is een statement opgenomen in de Gezamenlijke verwerkersverantwoordelijke overeenkomst
Deel 3 - Rechtenmatigheid		
Rechtsgrond		
21	Is van alle verwerkingen in kaart gebracht of een rechtmatige grondslag van toepassing is? Zo ja, geef aan elke rechtmatige grondslag van toepassing is, of welke grondslagen van toepassing zijn. Motiveer waarom die grondslag van toepassing is.	AvG art. 6 lid 1e, art. 9 lid 2j, art. 89 en art. 24 UAVG en wgbto 7:458. Het betreft een wetenschappelijk onderzoek naar de effectiviteit van bron- en contactonderzoek bij SARS-CoV-2 infectie. Retrospectief zijn er meer dan 2 miljoen testen gedaan in de corona teststraten en is bij honderduizenden bron- en contactonderzoek gedaan. De inspanning om aan deze betrokkenen achteraf toestemming te vragen is onevenredig.
22	Indien de verwerkingsactiviteiten zijn gebaseerd op het uitvoeren van een overeenkomst, geef aan om welke overeenkomst dit gaat en neem zo mogelijk een verwijzing naar de overeenkomst op.	Nvt
23	Indien de verwerkingsactiviteiten zijn gebaseerd op een wettelijke plicht, geef aan om welke wettelijke plicht dit gaat. Vermeld hierbij het wetsartikel.	Nvt
24	Indien de verwerkingsactiviteiten zijn gebaseerd op de vitale belangen van de betrokkene, geef aan om welke belangen dit gaat.	Nvt
25	Indien de verwerkingsactiviteiten zijn gebaseerd op 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, geef aan om welke taak dit gaat en noem het wetsartikel.	Nvt
26	Indien de verwerkingsactiviteiten zijn gebaseerd op een gerechtvaardigd belang, geef aan om welk belang dit gaat en beschrijf de afweging die hierbij is gemaakt.	nvt
27	Is de verwerking van bijzondere persoonsgegevens, strafrechtelijke persoonsgegevens en/of het BSN toegestaan? Geef aan waarom.	Ja, volgens AvG art. 9, 2j & UAVG artikel 24
Toestemming		
28	Indien de verwerkingsactiviteiten zijn gebaseerd op toestemming: is de toestemming vrij, specifiek, op informatie gebaseerd en onduidelijkheid gegeven door de betrokkene?	Nvt
29	Is de toestemming gegeven door middel van een duidelijke actieve handeling?	Nvt
30	Is of wordt bijgehouden hoe en wanneer de betrokkene toestemming heeft gegeven?	Nvt
31	Heeft de betrokkene de mogelijkheid om toestemming op ieder moment in te trekken en zonder negatieve gevolgen?	Nvt
32	Omvatten de verwerkingsactiviteiten websites, apps of andere online diensten van de informatie maatschappij gericht op/aangeboden aan kinderen onder de leeftijd van 16 jaar?	Nee
33	Wordt toestemming bij de situatie in de vorige vraag gevraagd door de persoon die ouderlijke verantwoordelijkheid voor het kind draagt?	Nvt
Transparantie		
34	Indien de persoonsgegevens direct bij de betrokkene worden verzameld; welke informatie wordt ten tijde van de verzameling gecommuniceerd?	CONTROL verzameld de gegevens niet direct bij de diensten, maar maakt gebruik van bestaande dataverzameling in het kader van de coronatest/bco keten.
35	Indien de persoonsgegevens niet direct bij de betrokkene worden verzameld; welke informatie wordt ten tijde van de verzameling (of ten minste binnen een maand na verkrijging) gecommuniceerd?	Er staat er op de website van de rijksoverheid over het beleid voor testen dat verder onderzoek op afgenomen materiaal door de GGD mogelijk is, en dat dit valt onder de geneeskundige behandelovereenkomst (https://www.rijksoverheid.nl/onderwerpen/coronavirus-covid-19/testen/testlocatie). Tevens staat er op de website van het RIVM met het landelijk geldende protocol voor Bron en Contactonderzoek welke data bewaard worden en dat deze gebruikt worden voor reguliere evaluatie, om waar nodig het beleid bij te stellen (https://lco.rivm.nl/COVID-19-bco). Tenslotte wordt er een samenvatting van het project gepubliceerd op de website van GGD Amsterdam. Daarnaast is er een samenvatting gepubliceerd op de website van ZonMW en zal de dataverzameling met beschrijving worden aangemeld bij een online repository. Ook staat er een algemene privacyverklaring op de website van de GGD Amsterdam (https://www.ggd.amsterdam.nl/ggd/privacyreglement/) en wordt een specifieke privacyverklaring voor CONTROL op de website van de GGD Amsterdam gepubliceerd (https://www.ggd.amsterdam.nl/beleid-onderzoek/projecten/)

36	Is het privacy statement geschreven in duidelijke bewoordingen en makkelijk vindbaar voor de betrokkenen?	Ja, deze staat op de algemene website van de GGD Amsterdam. Zie https://www.ggd.amsterdam.nl/ggd/privacyreglement/ & https://www.ggd.amsterdam.nl/beleid-onderzoek/projecten/
37	Indien de verwerking betrekking heeft op een samenwerkingsverband waarbij meerdere verwerkingsverantwoordelijken betrokken zijn, worden de relevante afspraken dan duidelijk gecommuniceerd aan de betrokkenen?	Ja, de Partijen sluiten een samenwerkingsovereenkomst en een gezamenlijke verwerkersovereenkomst waarin ook afspraken worden gemaakt over het informeren van Betrokkenen
Deel 4 - Rechten van betrokkenen		
38	Is bij het proces rekening gehouden met een effectieve uitoefening van het recht op inzage?	Ja, Conform artikel 8 uit de gezamenlijke verwerkers-verantwoordelijken overeenkomst wordt het recht op inzage gegeven door de Partij die de Betrokkene als eerste in de verwerking heeft opgenomen. Deze Partij verleent inzage in welke gegevens zijn verstrekt aan CONTROL. GGD Amsterdam geeft desgevraagd inzage in het gebruik van deze gegevens in analyses en rapportages. CONTROL kan personen niet met zekerheid identificeren in de onderzoeksdata. Voor verzoeken van Betrokkene(n) is een terugkoppeling nodig naar de GGD die zelf beschikt over de ruwe data.
39	Is bij het proces rekening gehouden met een effectieve uitoefening van het recht op rectificatie?	De Betrokkene dient zich te melden bij de Partij die de persoon als eerste in de verwerking heeft opgenomen (art. 8 gezamenlijke verwerkingsverantwoordelijken overeenkomst). Wijzigingen vinden plaats in de opgeslagen bronbestanden bij de lokale GGD. Daarna wordt opnieuw de pseudonisatie stap doorlopen en wordt het gewijzigde bestand geupload in de onderzoeksomgeving. Rectificatie direct in de onderzoeksomgeving is niet mogelijk.
40	Is bij het proces rekening gehouden met een effectieve uitoefening van het recht op wijziging/verwijdering van persoonsgegevens?	Idem
41	Kan worden voldaan aan een verzoek om dataportabiliteit?	Nvt
42	Is bij het proces rekening gehouden met een effectieve uitoefening van het recht op bezwaar?	Ja, Als Betrokkene(n) zich melden bij de Partij die deze als eerste in de verwerking heeft opgenomen en bezwaar maakt tegen gebruik dient deze Partij de Betrokkene te verwijderen uit de data en een nieuw bestand zonder deze gegevens te uploaden in anDREa. Zie ook #39
43	Is bij het proces rekening gehouden met een effectieve uitoefening van het recht op beperking?	Ja, conform route omschreven bij #39. De Partij waar de Betrokkene als eerste in de verwerking is opgenomen zorgt voor de wijzigingen in de databestanden.
44	Is de kwaliteit van de gegevens gewaarborgd, dat wil zeggen: zijn de gegevens actueel, juist en volledig	Ja, voor zover ze correct worden gerapporteerd in het corona proces. Kwaliteitstoetsing is geen onderdeel van CONTROL.
Profieling en geautomatiseerde besluitvorming		
45	Worden er profielen opgesteld van de betrokkenen, al dan niet geanonimiseerd?	Ja, er wordt een predictiemodel ontwikkeld om te bepalen welke personen een hoog risico hebben op het verspreiden van COVID-19, en voor wie het dus extra belangrijk is dat er snel en intensief bron en contactonderzoek uitgevoerd wordt.
46	Indien profielen worden opgesteld, kan het profiel tot uitsluiting of stigmatisering leiden?	Ja, mogelijk. Stel bijvoorbeeld dat 'maatschappelijk gevoelige' variabelen, zoals geboorteland, beroepsgroep, postcode/buurt voorspellend zijn voor een hoger risico op COVID transmissie, of voor een langere doorlooptijd van het BCO. Door wetenschappelijke publicatie van deze resultaten kan dit bekend worden. De bevindingen kunnen als stigmatiserend worden ervaren. Of dit in de praktijk zal optreden zal ten eerste afhangen van de onderzoeksresultaten, en ten tweede van of/hoe de resultaten naar buiten worden gecommuniceerd en/of hoe GGD/overheid de resultaten gebruiken om richtlijnen of werkinstructies aan te passen.
47	Is er sprake van geautomatiseerde besluitvorming? Zo ja, op basis van welke grondslag?	Nee. Dit predictiemodel kan door de uitvoerders van BCO als extra hulpmiddel gebruikt worden bij het prioriteren van casussen, maar het blijft altijd mensenwerk.
Deel 5 - Doelbinding & proportionaliteit		
48	Worden de persoonsgegevens gebruikt voor een ander doel dan waarvoor zij verzameld zijn?	Ja, in CONTROL worden de gegevens gebruikt om het corona test/BCO proces te evalueren en operationeel onderzoek te doen naar de effectiviteit van BCO in een wetenschappelijke setting. De gegevens zijn inbeel verzameld om zorg te kunnen leveren
49	Indien de vorige vraag met 'ja' is beantwoord: is het doel waarvoor de persoonsgegevens verwerkt gaan worden verenigbaar met het	Ja, zie genoemde grondslag in vraag 21. Het project evalueert het proces waarin de gegevens primair zijn verzameld.
50	Worden de persoonsgegevens gebruikt voor een ander doel dat niet specifiek is omschreven?	Nee
51	Is sprake van koppeling, verrijking of vergelijking van gegevens uit verschillende bronnen?	Ja, voor het project worden gegevens uit CoronIT gekoppeld aan de gegevens uit HPZone en GSIRIS. Dit gebeurt door de GGD'en zelf. CONTROL krijgt de gepseudonimiseerde gekoppelde dataset en voert zelf geen koppelingen uit.
52	Is de (voorgenomen) verwerking effectief om het beoogde doel te bereiken? Geef aan waarom.	Ja, het betreft geprotocolleerd procesonderzoek met duidelijk gedefinieerde onderzoeksvragen en methoden en een grote hoeveelheid data dus voldoende statistische power om deze vragen succesvol te beantwoorden.
53	Staat de impact voor de persoonlijke levenssfeer van de betrokkene van de voorgenomen verwerking van persoonsgegevens in redelijke verhouding tot het doel? Geef aan waarom.	Ja, de verwerking is noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid, zoals het waarborgen van hoge normen inzake kwaliteit en veiligheid van de gezondheidszorg en van geneesmiddelen of medische hulpmiddelen, op grond van Unierecht of lidstatelijk recht.
Deel 6 - Data minimalisatie & subsidiariteit		
54	Kan het proces ook worden gerealiseerd op een manier die minder ingrijpend is voor de impact op de privacy van betrokkenen? Geef aan waarom wel/niet.	Nee, het betreft een procesevaluatie van de werkelijkheid waarbij de data op individueel niveau die in de routineprocessen verzameld worden cruciaal zijn. Data zijn gepseudonimiseerd, rapportage van resultaten is geanonimiseerd.
55	Zijn alle persoonsgegevens noodzakelijk om het beoogde doel te bereiken?	Ja, omdat het gezien de uniciteit van deze pandemie vooraf niet te voorspellen is welke factoren het belangrijkst zullen zijn. Persoonsgegevens die niet gebruikt zullen worden in het project worden zsm na beëindiging verwijderd (zie sectie 2 verwerkersovereenkomst)
56	Hoe is geborgd dat de standaardinstellingen van de betrokken apparatuur of applicaties zodanig zijn dat alleen de persoonsgegevens worden verzameld die noodzakelijk zijn voor het specifieke doel? Geef aan welke maatregelen zijn getroffen.	CONTROL verzameld de data niet direct bij de betrokkenen, maar gebruikte bestaande databronnen. We maken gebruik van een data extractie handleiding. In de gezamenlijke verwerkersverantwoordelijken overeenkomst is een lijst opgenomen waarin expliciet staat vermeld welke variabelen we opnemen in CONTROL. Het verkrijgen van de data wordt zo ingericht dat er niet meer data dan benoemd worden verkregen dmv geautomatiseerde scripts die de GGD'en kunnen gebruiken voor het klaarmaken van de databestanden voor CONTROL.
Deel 7 - Opslagbeperkingen		

57	Worden de persoonsgegevens verwijderd op het moment dat zij niet meer noodzakelijk voor het bereiken van het doel?	Ja. Verwijdering van Persoonsgegevens gebeurt op diverse momenten in het project. Voor het uploaden van de data door de GGD'en in de onderzoeksomgeving vindt een pseudonisatie stap plaats en worden direct herleidbare persoonsgegevens verwijderd. Dit zijn naam, adres, telefoonnummer, emailadres, zorgverzekering. Er vinden diverse databewerkingen/coderingen plaats ter pseudonisatie, zoals geboortedatum omzetten in leeftijd. Identifiers worden verwijderd of gepseudoniseerd. CONTROL gebruikt gepseudoniseerde data. Een lijst met variabelen die behouden blijft voor onderzoek is opgenomen in de Gezamenlijke Verwerkersovereenkomst. De databewerkingen bij de GGD'en zijn vastgelegd in een handleiding en een script. In het data opschoningsproces in de Onderzoeksomgeving worden variabelen verwijderd die alsnog met zekerheid niet gebruikt zullen worden in onderzoek. Binnen 2 maanden na beëindiging van het onderzoeksproject worden alle data die niet zijn gebruikt in rapportages en/of (wetenschappelijke) publicaties verwijderd. Data die wel zijn gebruikt worden gearchiveerd voor 5 jaar.
58	Op welke manier wordt gerealiseerd dat de data daadwerkelijk worden verwijderd/geanoniseerd?	Data worden bewaard conform bewaartermijn (zie overeenkomst § 8 #57). Vernietiging van data wordt gedaan door 5.1.2e of de 5.1.2e zij zijn ook de enigen die hier toe gemachtigd zijn in de Onderzoeksomgeving. Na vernietiging/verwijdering van gegevens wordt de eigenaar van de data (een of meerdere Partners) hiervan per email op de hoogte gesteld. De procedure van het verwijderen/vernietigen van data is vastgelegd in de Gezamenlijke verwerkersverantwoordelijke overeenkomst.
59	Indien geen bewaartermijnen zijn gedefinieerd, zijn er maatregelen genomen om de persoonsgegevens desalniettemin te verwijderen?	Nvt
Deel 8 - Beveiliging, integriteit en vertrouwelijkheid		
60	Zijn er op basis van de VRA extra maatregelen nodig, naast de BIG maatregelen?	Zie tabblad advies 1.2e Advies wordt overgenomen in de verwerkersovereenkomst met andREa, de cloud omgeving
61	Is voor dit proces aangesloten bij een goedgekeurde gedragscode? Zo ja, vermeld de gedragscode.	Ja. In artikel 9 van de samenwerkingsovereenkomst staan de gedragscodes genoemd waar we ons binnen dit project aan conformeren. De volgende tekst is opgenomen in de Samenwerkingsovereenkomst 1. Partijen conformeren zich aan de Nederlandse Gedragscode Wetenschappelijke Onderzoek, de Gedragscode voor Gezondheidsonderzoek ("Code Goed Gedrag"), de Code ter Voorkoming van Oneigenlijke Beïnvloeding door Belangenverstrengeling en de Nederlandse Gedragscode Wetenschappelijke Integriteit 2018. 2. Partijen verklaren deze codes in het kader van dit Project te onderschrijven en zullen niets ondernemen in het kader van dit Project in strijd met deze codes.
62	Zijn de persoonsgegevens gepseudoniseerd waar mogelijk?	Ja, de GGD'en uploaden een gepseudoniseerd databestand aan CONTROL.
63	Zijn de persoonsgegevens versleuteld waar mogelijk?	Ja, transfer en opslag zijn encrypted
64	Zijn toegangsmaatregelen genomen waardoor alleen personen toegang hebben tot persoonsgegevens voor zover dat noodzakelijk is voor de uitoefening van hun taak?	Ja. De stuurgroep van het project bestaat uit 1 lid van elke Partij alsmede 5.1.2e Zij bepalen wie toegang krijgen tot de verschillende delen van de data. Per GGD is er één persoon aangewezen (dit is een data manager of onderzoeker) die beperkte rechten krijgt voor toegang tot de Onderzoeksomgeving. Met deze rechten kunnen data alleen geload worden, reeds aanwezige data kan niet ingezien of gedownload worden. Deze personen tekenen een gebruikersovereenkomst waarin zij akkoord gaan met de overeengekomen rechten, plichten en voorwaarden. Verder kan een persoon toegang tot de data krijgen als onderzoeker. Hiervoor dient die persoon een verzoek in bij 5.1.2e die dit voorlegt en akkoord vraagt aan de stuurgroep. Onderzoekers krijgen bredere toegang, namelijk tot het openen van de data om analyses uit te voeren. Ook onderzoekers tekenen een gebruikersovereenkomst 5.1.2e monitort de logbestanden van de toegang en het gebruik van de Onderzoeksomgeving en deelt bevindingen in de stuurgroep overlopen. Bij ongewenst gebruik worden rechten ingetrokken. De Onderzoeksomgeving is beveiligd tegen ongeoorloofd downloaden en vernietigen van data door personen anders dan 5.1.2e en 5.1.2e Voor alle personen geldt dat toegang tot de Onderzoeksomgeving werkt met een twee factor authenticatie om het risico op toegang door onbevoegden verder te verkleinen.
Deel 9 - Beschrijving en beoordeling risico's betrokkenen		
65	Omschrijf welke negatieve privacy gevolgen voor betrokkenen mogelijk kunnen optreden bij de uitvoering van dit proces.	Wanneer een client positief test op corona wordt er een uitvoerig bron- contactonderzoek gedaan waarmee inzicht verkregen wordt in de persoonlijke sfeer van de Betrokkene. Deze data worden gebruikt in CONTROL. De combinatie van specifieke gegevens maakt de Betrokkene mogelijk herleidbaar, al worden duidelijk identificerende gegevens direct verwijderd. Er is een kleine kans op discriminatie/stigmatisering/uitsluiting en relationele schade als een Betrokkene geïdentificeerd wordt. Omdat de data enkel ingezien kan worden door een klein en door ons gecontroleerd groepje gebruikers is de kans op negatieve gevolgen zeer klein. Echter, een datablek valt nooit 100% uit te sluiten, en in het geval van een datablek is de kans op negatieve privacy gevolgen groter.
66	Hoe groot is de kans dat de omschreven risico's zich voordoen?	Klein, want 1) transfer en opslag van data is encrypted en gebeurt in een veilige omgeving, 2) toegangsrechten worden actief uitgegeven en gemonitord alleen aan die personen voor wie het noodzakelijk is, 3) data worden niet langer opgeslagen dan noodzakelijk, 4) data zijn niet direct herleidbaar, maar alleen in combinatie en 5) er worden samenwerkings-, verwerkers en gebruikersovereenkomsten afgesloten met Partijen en individuen die toegang krijgen tot data
67	Omschrijf het restrisico voor de betrokkenen. Geef aan of dit restrisico hoog is.	Niet anders dan hierboven beschreven
68	Omschrijf de voorgestelde maatregelen om het restrisico te mitigeren.	Alle aanvullende maatregelen worden benoemd in het tabblad Risico's + maatregelen.
Deel 10 - Ingewonnen advies		
69	Is er advies ingewonnen van 5.1.2e bij het uitvoeren van deze DPIA?	Ja, zie tabblad Advies 1.2e Advies van 5.1.2e is verwerkt in deze versie van de DPIA.
70	Is er advies ingewonnen van de Autoriteit Persoonsgegevens bij het uitvoeren van deze DPIA? Geef aan waarom wel of geen advies is ingevonnen.	Nee, er is advies ingewonnen bij 5.1.2e van de Gemeente Amsterdam (zie tabblad) en 5.1.2e van GGD Zuid-Limburg. Er is geen twijfel over het uit te voeren project. Advies van 5.1.2e is verwerkt in deze versie van de DPIA.
71	Indien advies is ingewonnen van de Autoriteit Persoonsgegevens, geef aan op welke manier invulling is gegeven aan dit advies.	Nvt
72	Is de betrokkenen (of hun vertegenwoordigers) gevraagd om hun visie te geven over de verwerkingsactiviteiten? Geef aan waarom wel/niet.	Nog niet, maar dat wordt tijdens het project wel gedaan door vertegenwoordigers van de cliënten op te nemen in de adviesgroep
73	Geef aan op welke manier opvolging is gegeven aan de visie van betrokkenen. Indien geen opvolging is gegeven aan deze visie, motiveer waarom dat niet is gedaan.	Nvt

Risico's & maatregelen

Welke negatieve privacy gevolgen voor betrokkenen kunnen mogelijk optreden?	Voorgestelde maatregelen?
Pseudonimisatie stap bij een Partij verloopt niet goed en data met direct herleidbare gegevens worden geupload in de digital research environment	Data transfer en opslag is encrypted. Er is een handleiding opgesteld waarin de extractie, pseudonimisatie en het uploaden van data tot in detail wordt omschreven. Ook is een R script opgesteld die de stappen van koppeling en pseudonimisatie uitvoert. In de handleiding is opgenomen dat bestanden tussen genereren en uploaden dienen te worden gecheckt. Mocht het alsnog gebeuren dat onvoldoende gepseudonimiseerde data worden geupload dan wordt een verzoek tot verwijdering van de gegevens gedaan bij de DRE zo spoedig mogelijk nadat het is opgemerkt en het datalek wordt gemeld. Het aantal personen dat in dit geval toegang heeft kunnen hebben is beperkt tot die personen die de rechten hebben om in te loggen in de cloud als onderzoeker. In de log is te achterhalen wie de persoonsgegevens heeft ingezien.
Niet geautoriseerde personen krijgen toegang tot de data in de DRE	Toegangsrechten worden aangevraagd bij de Projectleider. Gebruikersvoorwaarden dienen ondertekend te worden. De projectleider vraagt accounts aan bij de DRE en monitort toegang actief. Elk kwartaal wordt de log bekeken waarin is bijgehouden wie toegang heeft gehad en heeft probeerd te krijgen tot de DRE. Bij oneigenlijk gebruik wordt een account verwijderd. De data zijn extra beveiligd tegen verwijderen en downloaden. Wanneer dit wordt geprobeerd wordt direct een email gestuurd aan de projectleider en data steward die toestemming moeten geven voor deze handeling alvorens hij kan worden uitgevoerd.
Diverse technische risico's van de DRE	De research cloud heeft vele voorzorgsmaatregelen getroffen om datalekken te voorkomen, zoals toegangsbeheer, twee-factor authenticatie, geen internet of email binnen de digitale omgeving, etc. Zie voor meer details de bijlage: DPIA anDREa vs 1.0, augustus 2020
Het gebruik van cloud technologie voor data-uploads, data-opslag en analyse kan leiden tot een datalek	De research cloud heeft vele voorzorgsmaatregelen getroffen om datalekken te voorkomen, zoals toegangsbeheer, twee-factor authenticatie, geen internet of email binnen de digitale omgeving, etc. Zie voor meer details de bijlage: DPIA anDREa vs 1.0, augustus 2020
Het verwerken van bijzondere persoonsgegevens.	We treffen een aantal beveiligingsmaatregelen om risico's zoveel mogelijk in te perken die ook zijn genoemd in de DPIA. Dit zijn: 1) Pseudonimisatie om de kans op herleidbaarheid te verminderen. Data worden door de GGD'en gepseudonimiseerd voordat de data worden geupload in de cloud omgeving voor het onderzoek. Als beveiligingsmaatregel bieden we vanuit het project de procedure voor pseudonimisatie aan, waardoor het risico dat er toch direct herleidbare persoonsgegevens worden geupload tot een minimum wordt beperkt. Door de pseudonimisatie zijn de records in de dataset zijn niet direct herleidbaar. Er kan sprake zijn van indirecte herleidbaarheid door de hoeveelheid en combinatie van variabelen. 2) Codering van gevoelige variabelen zoals geboorteland en bezochte religieuze plaats. Hierdoor is de betekenis van de waarde in cellen niet direct te interpreteren. De variabelen die worden gecodeerd zijn geïdentificeerd in bijlage 5 van de gezamenlijke verwerkersverantwoordelijke overeenkomst

	3) Strikte toegangsregulatie tot de cloud-omgeving waar de data worden opgeslagen. Toegang hebben de projectleider, data steward van het project. Zij kunnen data managers (die alleen data kunnen uploaden, maar niet inzien) en onderzoekers (die data mogen inzien/analyseren) aanmelden voor toegang. Dat betekent dat slechts een beperkt aantal mensen, namelijk de projectleider, data steward en
het gebruik van data van kwetsbare personen kan voor hen een groter risico opleveren op de negatieve gevolgen van een mogelijk datalek	Ten eerste hanteren we veel algemene voorzorgsmaatregelen, zoals die omschreven in de DPIA van het anDREa systeem, waarmee het risico op datalekken voor iedereen, en dus ook kwetsbare personen, beperkt wordt. Ten tweede gebruiken we alleen gepseudonimiseerde data en coderen we potentieel gevoelige informatie. Kwetsbaarheid kan in veel gevallen door ons niet worden achterhaald, omdat deze informatie niet in de dataverzameling is opgenomen.
Grote hoeveelheid participanten	Gezien de vele beveiligingsmaatregelen die er voor het omgaan met de data reeds genomen worden geeft het grote aantal personen in de dataset geen aanleiding tot verdere maatregelen.
Samenwerking met externe partijen	Voor de samenwerking met de andere GGD'en en het RIVM is een samenwerkingsovereenkomst opgesteld. Tussen de GGD'en is ook geen gezamenlijke verwerkersverantwoordelijken overeenkomst opgesteld die duidelijk omschrijven wat eenieders verantwoordelijkheden, verplichtingen, en rechten zijn.
Informeren van betrokkenen	Gezien de data in het kader van het zorgproces op zeer grote schaal verzameld worden, is het voor de onderzoekers niet mogelijk alle Betrokkenen te informeren. Er wordt wel een samenvatting van het project gepubliceerd op de website van GGD Amsterdam. Daarnaast is er een samenvatting gepubliceerd op de website van ZonMW en zal de dataverzameling met beschrijving worden aangemeld bij een online repository. CONTROL gebruikt retrospectief verzamelde data.
Mogelijkheid tot inzage/rectificatie/verwijdering	Betrokkene(n) hebben het recht op inzage, rectificatie en verwijdering van hun gegevens die worden gebruikt in CONTROL. Het proces om dit te bewerkstelligen is omslachtig. CONTROL kan in de onderzoeksomgeving personen niet herleiden, omdat pseudonimisatie plaatsvindt lokaal bij de GGD'en. De GGD'en moeten daarom de bronbestanden die ten grondslag liggen aan het gepseudonimiseerde bestand dat wordt verstrekt aan CONTROL archiveren. Inzage, rectificatie en verwijdering kan plaatsvinden vanaf dit bestand. Wanneer wijzigingen zijn aangebracht dient een nieuw bestand geupload te worden in de cloud en worden de wijzigingen overgenomen in de onderzoeksdatabase.
Kwaliteit van de (bron)gegevens	We gebruiken enkel data die in het kader van reguliere zorg worden ingevoerd. Aan de kwaliteit van de brondata kunnen wij dus niets veranderen. Wat we wel doen is harmoniseren van data uit de verschillende systemen en regio's voordat het samengevoegd wordt om eventuele problemen ten gevolge van verschillen in invoer te voorkomen. Tevens is de beoordeling van het proces een belangrijk doel van het onderzoek, dus zou een mindere kwaliteit van data invoer een uitkomst kunnen zijn om verder te onderzoeken.

Profilerings (De onderzoeksresultaten kunnen aanleiding geven tot discriminatie van bevolkingsgroepen)	Een van de doelen is het maken van een predictiemodel om te kunnen voorspellen welke personen een hoog risico hebben om het virus te verspreiden, en dus een hoge prioriteit hebben om snel en intensief bron en contactonderzoek uit te voeren. Dit zal echter nooit op persoonlijk niveau gebeuren, maar altijd op geaggregeerd niveau. Echter, het behoren tot een groep die als hoog risico benoemd wordt (bijv. wonend in een bepaald stadsdeel) kan mogelijk als stigmatiserend beschouwd worden. Echter, dit onderzoek beperkt zich tot het ontwikkelen van dat model, niet tot het gebruik ervan. In het gebruik gebruik van een dergelijk predictiemodel, en met name in de communicatie daarover zal er uiterst zorgvuldig gehandeld worden om het risico op stigmatisering te beperken. Als de resultaten daar aanleiding toe geven kan ook contact gezocht worden met de (hoog risico) groep in kwestie alvorens de resultaten openbaar gemaakt worden.
Gegevens worden verwerkt voor een ander doel dan waarvoor ze verzameld zijn	De gegevens worden verzameld in het kader van zorgverlening, en door ons gebruikt in het kader van onderzoek. Echter, doordat het doel van ons onderzoek is om de zorgverlening te optimaliseren, kan gesteld worden dat ons onderzoek wel in de lijn ligt van het oorspronkelijke doel. Tevens proberen we door niet meer variabelen dan nodig te gebruiken, en door pseudonimering de mogelijke impact voor de personen wiens data gebruikt wordt te beperken.
Koppeling systemen	De databronnen die binnen ons onderzoek gebruikt worden en waarvan de geëxporteerde datasets aan elkaar gekoppeld worden zijn sterk verwant. In CoronIT staan gegevens over het aanvragen en uitvoeren van een COVID-19 test, en voor iedereen die positief test wordt dit automatisch doorgezet naar HPZone, het systeem waar de informatie uit het bron en contactonderzoek ingevoerd wordt. OSIRIS heeft overlap met HPZone data, maar is beter gestructureerd. De koppelingen worden nu in het reguliere zorgproces ook al gemaakt, dus het koppelen in het kader van dit onderzoek is niet dermate risicovol dat het aanleiding geeft tot verdere maatregelen. We benadrukken dat er geen koppeling plaatsvindt tussen de data van de verschillende GGD'en.
Kans op stigmatisering van geïdentificeerde groepen	Alvorens gevoelige resultaten naar buiten worden gebracht wordt communicatie hierover afgestemd met de afdeling communicatie van tenminste de GGD Amsterdam en is goedkeuring van de CONTROL stuurgroep nodig. Regels rondom publicatie van gegevens zijn opgenomen in de consortiumovereenkomst.
De data bestaat voor een deel uit tekstvelden. Hierin kunnen persoonsgegevens voorkomen.	Omdat deze tekstvelden ook waardevolle informatie bevatten voor het project zijn deze velden wel noodzakelijk. Omdat het niet de bedoeling is om direct herleidbare gegevens te bewaren binnen CONTROL zullen we direct na het uploaden van data deze velden onderzoeken. Dit betreft in ieder geval de 'diagnostic notes'. Relevante data worden uit dit veld geëxtraheerd, waarna het veld 'diagnostic notes' uit de data wordt verwijderd. We onderzoeken ook of deze procedure nodig is voor andere tekstvelden in de data.

Doelen en verwerkingen

Nr.	Verwerking	Categorie persoonsgegevens	Type persoonsgegevens
	[omschrijving van de verwerking]	[welke persoonsgegevens worden er gebruikt voor deze verwerking? Bijv. Naam, adres, woonplaats, telefoonnummer, locatie, klantnummer etc.]	[Normaal, gevoelig, en/of bijzonder]
1	Data extractie uit HPZone (Deze verwerking is eigenlijk geen onderdeel van CONTROL. CONTROL start met het uploaden van gepseudonimiseerde data naar de cloud. Om de kwaliteit en veiligheid van deze data te borgen heeft CONTROL een handleiding en script ontwikkeld waarmee de data extractie uit de bronsystemen gedaan kan worden)	Achternaam, postcode-6, leeftijd, gezondheidsgegevens, geboorteland, beroep, locaties, contacten	Bijzonder
2	Data extractie uit CoronIT (Deze verwerking is eigenlijk geen onderdeel van CONTROL. CONTROL start met het uploaden van gepseudonimiseerde data naar de cloud. Om de kwaliteit en veiligheid van deze data te borgen heeft CONTROL een handleiding en script ontwikkeld waarmee de data extractie uit de bronsystemen gedaan kan worden)	Achternaam, postcode-6, leeftijd, gezondheidsgegevens (symptomen, reden test, testuitslag, testdatum)	Normaal
3	GGD'en vragen de OSIRIS data op bij het RIVM. (Deze verwerking is geen onderdeel van CONTROL. CONTROL start bij het uploaden van de data naar de cloud. Deze verwerking is opgenomen in de lijst om aan te geven waar de CONTROL data vandaan komen)	Data zijn gepseudonimiseerd. Gestructureerd verzamelde gezondheidsgegevens	Normaal
3	Databestand maken door koppelen van data uit HPZone, CoronIT en OSIRIS (Deze verwerking is eigenlijk geen onderdeel van CONTROL. CONTROL start met het uploaden van gepseudonimiseerde data naar de cloud. Om de kwaliteit en veiligheid van deze data te borgen heeft CONTROL een handleiding en script ontwikkeld waarmee de data kunnen worden gekoppeld)	Naam, postcode-6, leeftijd, OSIRISnummer, gestructureerde gezondheidsgegevens uit HPZone	Bijzonder
4	Databestand pseudonimiseren & verwijderen zoveel mogelijk persoonsgegevens (Deze verwerking is eigenlijk geen onderdeel van CONTROL. CONTROL start met het uploaden van gepseudonimiseerde data naar de cloud. Om de kwaliteit en veiligheid van deze data te borgen heeft CONTROL een handleiding en script ontwikkeld waarmee de data extractie uit de bronsystemen gedaan kan worden)	Na pseudonimisatie zijn de overgebleven persoonsgegevens: postcode-4, gezondheidsgegevens, geboorteland, beroep, locaties, contacten.	Bijzonder
5	Databestand uploaden naar DRE	postcode-4, gezondheidsgegevens, geboorteland, beroep, locaties, contacten	Bijzonder

6	Databestanden Partijen opslaan in SQL database in DRE, data bewerken voor analyse en analyseren	postcode, gezondheidsgegevens, geboorteland, beroep, locaties, contacten	Bijzonder
7	Verwijderen gegevens uit de DRE	postcode, gezondheidsgegevens, geboorteland, beroep, locaties, contacten	Bijzonder

Nr.	Categorie betrokkenen	Doel	Applicatie
	[van wie worden gegevens verwerkt? Bijvoorbeeld: inwoners, medewerkers, vergunninghouders etc]	[geef aan waarom de gegevens worden verwerkt]	[noem eventueel een gebruikt applicatie]
1	Inwoners in de GGD regio's Amsterdam, Rotterdam-Rijnmond, Gelderland-Midden, Groningen, Zuid Limburg, Flevoland, Regio Utrecht, Hart voor Brabant	De verwerkingen tezamen hebben als doel wetenschappelijk operationeel onderzoek te doen naar de corona testketen en het bron- en contactonderzoek bij de samenwerkende Partijen. De bron- en contact data zijn opgeslagen in HPZone en om deze te kunnen bekijken/analyseren dienen ze hieruit geëxtraheerd te worden.	HPZone
2	Idem	De verwerkingen tezamen hebben als doel wetenschappelijk operationeel onderzoek te doen naar de corona testketen en het bron- en contactonderzoek bij de samenwerkende Partijen. Testketen data zijn opgeslagen in CoronIT en om deze te kunnen bekijken/analyseren dienen ze hieruit geëxtraheerd te worden.	CoronIT
3	Idem	De verwerkingen tezamen hebben als doel wetenschappelijk operationeel onderzoek te doen naar de corona testketen en het bron- en contactonderzoek bij de samenwerkende Partijen. De bron- en contact data zijn opgeslagen in HPZone en om deze te kunnen bekijken/analyseren dienen ze hieruit geëxtraheerd te worden.	Nvt
3	Idem	Coronadata van een persoon worden opgeslagen in 3 bronnen. Om een totaalbeeld te krijgen van het corona test/bco proces dienen deze bronnen aan elkaar gelinkt te worden	R of R studio
4	Idem	Een deel van de persoonsgegevens zijn alleen nodig voor het uitvoeren van de koppeling en kunnen daarna verwijderd worden	R of R studio
5	Idem	De data van de GGD'en worden gezamenlijk opgeslagen in een data warehouse en gezamenlijk geanalyseerd door onderzoekers die deze bevoegdheid van de stuurgroep hebben gekregen. Het is daarom nodig dat databestanden bij elkaar worden gebracht in 1 groot datawarehouse	Digital Research Environment (DRE) van anDREa

6	Idem	Voor de analyse van data is het nodig dat er data bewerkingen uitgevoerd worden (zoals het categoriseren van data). Hierdoor worden de data minder herleidbaar en bruikbaar voor statistische analyses.	anDREa
7	Idem	Na afloop van het project worden de gegevens verwijderd	anDREa

DPIA advies		5.1.2e	Amsterdam
Punt	Opmerkingen	5.1.2e	Reactie
10	Verwerking van bijzondere gegevens, zijn hier extra beveiligingsmaatregelen voor getroffen?		Ja, deze maatregelen zijn beschreven in tabblad Risico's + maatregelen
12	Onduidelijk wat bedoeld wordt met: 'de dataverzameling bevat geen brondata en heeft in die zin geen bewaartermijn'		De beantwoording van dit punt is aangepast, om aan te geven dat de bewaarplicht voor de primaire data niet onder ons project valt, en ook wat wij als bewaartermijn hanteren voor de door ons gebruikte data.
16	Tussen de GGD/RIVM geldt waarschijnlijk een convenant. De andere verwerkersovereenkomst klopt.		De beantwoording van dit punt is aangepast, om duidelijker aan te geven hoe de samenwerking tussen verschillende partijen in het project vastgelegd is.
18	Zijn deze verwerkersovereenkomsten nagekeken?		De verwerkersovereenkomst is naar een van de PO's gestuurd, maar er is nog geen reactie op ontvangen. Het is nu opnieuw als bijlage bijgevoegd.
23	Duidelijke grondslag maar welk wetsartikel is van toepassing?		De beantwoording van dit punt is aangepast, om specifieker aan te geven op welke artikelen in de betreffende wet de grondslag gebaseerd is.
31	Waar kan de betrokkene deze vinden? En is dit voor de betrokkene duidelijk?		De beantwoording van punt 31 en punt 35 zijn aangepast om meer uitleg te geven over de verschillende kanalen waardoor de betrokkenen geïnformeerd worden over het gebruik van hun data voor onderzoek.
41	In dit geval is dit recht niet van belang.		De beantwoording is aangepast, om te benadrukken dat dit niet van toepassing is.
57	Hoe gaat dit in z'n werk? Hoe en welke gegevens worden wanneer verwijderd?		De beantwoording is aangepast, er is een gedetailleerde beschrijving toegevoegd van de werkwijze voor het verwijderen van data op verschillende momenten in het proces.
61	Een gedragscode is wat anders dan een samenwerkingsovereenkomst. Het gaat hier bijv. om wetenschappelijke/ gezondheids gedragscodes.		De beantwoording is aangepast, om duidelijk te maken dat de samenwerkingsovereenkomst rechtstreeks verwijst naar een aantal gedragscodes waar we ons binnen het project aan conformeren.

64	Is er een autorisatiebeleid hiervoor?	Ja, de beantwoording is aangepast om in meer detail te beschreven welk autorisatiebeleid er gehanteerd wordt.
68	Niet afdoende, graag iets meer maatregelen benoemen.	Alle aanvullende maatregelen worden besproken in tabblad Risico's + maatregelen, daar wordt in de beantwoording van dit punt nu ook specifiek naar verwezen.

DPIA advies 5.1.2e Amsterdam

#	Advies (zwart) & reactie op advies (blauw)
Algemeen	1. Het gaat om een evaluatie van het bron- en contact onderzoek i.v.m. Covid 19 waarbij op grote schaal naast gewone, tevens gevoelige en bijzondere persoonsgegevens zullen worden verwerkt. Beschrijf duidelijk welke persoonsgegevens noodzakelijk zijn om onderzoek te doen naar de effectiviteit van bron- en contact onderzoek i.v.m. Covid 19 én waarom deze persoonsgegevens daarvoor noodzakelijk zijn. Uitleg bij vraag 55 kan niet mee worden volstaan. Gelet op de hoeveelheid en gevoeligheid van betrokken persoonsgegevens is nadere onderbouwing noodzakelijk. 2. Geef aan of de gebruikte cloud oplossing is beoordeeld vanuit security perspectief en wat daaruit is gekomen. Geef tevens aan wat voor type cloud gebruikt zal worden voor dit onderzoek (public, hybrid, private). 1. In bijlage 5 van de verwerkersovereenkomst is een lijst met variabelen opgenomen die worden geëxtraheerd. De onderbouwing wordt in deze bijlage per variabele gegeven. 2. 5.1.2e heeft check uitgevoerd. BIA en Advies 5.1.2e zijn toegevoegd als tabbladen in deze DPIA. Maatregelen van 5.1.2e worden overgenomen in de verwerkersovereenkomst met anDREa
Tabblad 'DPIA', vraag 9	Geef aan hoe de volgende gegevens worden verkregen: geboorteland, beroep en ethniciteit. Licht toe waarom deze van belang zijn voor het onderzoek Geef aan waarom hier de OSIRIS data ontbreekt De GGD medewerker die het bron- en contactonderzoek uitvoert vraagt waar de betrokkene is geboren en welk beroep deze heeft. Er was bij ons een misverstand mbt ethniciteit. Er blijkt geen gedetailleerdere informatie over ethniciteit te worden uitgevraagd. Alleen het geboorteland van betrokkene zelf is bekend. In het onderzoek evalueren we de effectiviteit van het BCO. De kwaliteit van het BCO is daarin belangrijk. Het is zeker niet op voorhand uit te sluiten dat er een associatie is tussen geboorteland van de client en de kwaliteit van het BCO, doordat er bijvoorbeeld een taalbarriere is. Conclusies over de associatie moeten voorzichtig getrokken worden en op geen enkele wijze aanleiding geven tot discriminatie, maar wel het BCO optimaliseren. Zie toevoeging tabblad 'Risico's + maatregelen' 16. Beroep is noodzakelijk, omdat we weten dat verspreiding van het virus in bepaalde settings (bv vleesverwerkingsbedrijven of zorginstellingen) veel voorkomt of extra zorgelijk is. Dit zijn indicatoren die worden gebruikt om te bepalen of het een 'risico BCO' is of niet. En dit is bepalend voor de mate van detail die wordt uitgevraagd. Voor het onderzoek is beroep een verklarende factor voor de kwaliteit van het uitgevoerde BCO. De OSIRIS data bevat een zeer selecte hoeveelheid van BCO gegevens die de GGD'en per client sturen aan het RIVM voor landelijke surveillance. In deze set zijn de genoemde variabelen niet opgenomen
Tabblad 'DPIA', vraag 10	Zie vrg. 9. Geef aan waarom religie van belang is of zou kunnen zijn voor dit onderzoek. Religie is op zichzelf geen variabele waarin we binnen CONTROL geïnteresseerd zijn. Het is bijvangst omdat we wel geïnteresseerd zijn in de locaties die clienten in de infectieuze periode hebben bezocht. Deze locaties worden tijdens het BCO uitgevraagd, het is mogelijk dat hierbij een religieuze organisatie genoemd wordt. Wij willen dan wel mensen kunnen linken aan die locatie, maar daarbij is het voor ons niet van belang te weten om welke religie het gaat. Als extra maatregelen nemen we op dat religieuze locaties worden gecodeerd als religieuze locatie ##, waardoor de religie niet af te leiden is (zie extra maatregel 16)
Tabblad 'DPIA', vraag 11	Geef aan uit welke gegevens religie kan worden afgeleid. Geef aan hoe religie op objectieve wijze uit deze gegevens zou kunnen worden afgeleid. Uit de locaties die clienten in de infectieuze periode hebben bezocht. Deze locaties worden tijdens het BCO uitgevraagd. Wanneer hier een religieuze instelling/locatie benoemd wordt, kan dat informatie geven over de religie van de persoon in kwestie. Daarom zullen we direct na het verkrijgen van de data deze locaties coderen tot 'religieuze locatie #1' etc (zie toevoeging in maatregel 6).
Tabblad 'DPIA', vraag 12	College van B&W is bestuurlijk verantwoordelijk Aangepast

Tabblad DPIA, vrg 1	(1) Licht toe wat de rol is van het RIVM. (2) Licht toe hoe de datauitwisseling uit de consortiumovereenkomst kan worden weggelaten. Op basis van de DPIA, dit ziet op de kern van de samenwerking. De consortiumovk zou kunnen worden gezien als een gezamenlijke verwerkingsovereenkomst. Hierin moeten juist afspraken worden gemaakt mbt de data-verstrekking. 1) Het RIVM is een van de samenwerkende partners in dit project. We werken obv gelijkheid samen aan het onderzoek. Taken/bijdragen/verwachtingen zijn vastgelegd in de consortiumovereenkomst. Elke GGD deelt vanuit de eigen data-systemen die in het kader van reguliere COVID-zorg worden ingevuld een subset van die data met het RIVM voor landelijke surveillance (de OSIRIS data). Vanwege de structuur van die systemen is het niet (altijd) mogelijk voor de GGD'en om die specifieke subset ook weer uit de eigen data te exporteren en in te zien/gebruiken. Maar omdat het hier verplichte velden betreft is juist die data vaak van betere kwaliteit, en daarmee essentieel voor het uitvoeren van ons onderzoek. Door het RIVM als partner in het onderzoek te hebben, kunnen wij toegang krijgen tot die data. 2) De overeenkomsten die in CONTROL zijn opgesteld zijn een consortiumovereenkomst en een verwerkersovereenkomst. In de consortiumovereenkomst hebben we afspraken gemaakt over de wijze van samenwerking, communicatie met elkaar en naar buiten en financiën. In de verwerkersovereenkomst hebben we de afspraken gemaakt over het gebruik van data, de uitwisseling en beveiliging. Dit is conform werkwijze GGD en advies 5.1.2e De tekst in de DPIA was onnodig verwarrend en is daarom aangepast.
Tabblad 'DPIA', vrg	Geef aan waarom deze partijen verwerkers zijn. Oi kwalificeert de GGD Amsterdam als verwerker voor de gezamenlijk verwerkingsverantwoordelijken. Met de GGD Amsterdam moeten de overige partijen een verwerkersovereenkomst afsluiten GGD Amsterdam is verwerker, omdat wij gepseudonimiseerde data ontvangen van de andere GGD'en en deze analyseren. De andere GGD'en pseudonimiseren de data, voeren enkele andere databewerkingen uit en uploaden de data in de cloud. In de verwerkersovereenkomst zijn ieders specifieke verantwoordelijkheden vastgelegd. De overige GGD'en moeten inderdaad met ons een verwerkersovereenkomst afsluiten. Als gezamenlijke partners in het project hebben we ervoor gekozen dat wij vanuit Amsterdam dit document opstellen en met input van alle Partijen tot 1 gezamenlijke verwerkersovereenkomst komen
Tabblad 'DPIA', vra	zie opmerkingen bij vrg. 16 & 17 Zie antwoord C8 en C9
Tabblad 'DPIA', vra	Artikel 6 lid 1 sub c Wet publieke gezondheid ziet op het uitvoeren van bron- en contactonderzoek, niet op onderzoek naar de effectiviteit ervan. De wettelijke verplichting is het uitvoeren van het bron- en contactonderzoek. Om deze taak goed uit te voeren is het belangrijk deze processen ook te evalueren en te optimaliseren en dus na te gaan of we de taak ook goed uitvoeren. Evaluatie van kwaliteit/effectiviteit lijkt ons onlosmakelijk verbonden met het uitvoeren van de taak op zich.
Tabblad 'DPIA', vra	Leg uit waarom de volgende artikelen relevant zijn als grondslag voor het voorgestelde onderzoek en daarbij betrokken verwerkingen: artikelen 34 (opname ter isolatie in een zh), 47 (gebouwen, terreinen, goederen, vervoermiddelen controleren zonodig door het nemen van monsters), 51 (schip, luchtvaartuig), 54 (burger(lucht)haven), 55 (vervoerexploitant) of 56 (certificaat van sanitaire controle) Wet publieke gezondheid. Deze artikelen zijn onterecht aangehaald. We hebben contact gehad met 5.1.2e De grondslag voor CONTROL is artikel 24 van de UAVG. Dit hebben we aangepast. Op enkele punten in de DPIA noemen we nog wel artikel 6.1 – het uitvoeren van BCO - omdat dit het primaire proces is dat CONTROL evalueert.
Tabblad DPIA, vrg 3	Dit antwoord kan worden verplaatst naar vrg 34(transparantie.) Antwoord is verplaatst
Tabblad DPIA, vrg 3	Zie 31 en 35 Antwoord is verplaatst
Tabblad DPIA, vrg 3	Dit antwoord kan worden verplaatst naar vrg. 34 Antwoord is deels verplaatst

Tabblad DPIA, vrg 4	dataportabiliteit is in dit kader nvt Antwoord is aangepast naar nvt
Tabblad DPIA, vrg 4	zie opmerkingen bij vrg 9. Gezien de gevoeligheid moet dit worden afgedicht. Geef aan wat met prioritering wordt bedoeld. Er is duidelijker omschreven wat bedoeld wordt met prioritering, en in meer detail aangegeven in welke situaties dit zou kunnen optreden. Daarmee wordt beschreven dat of die prioritering plaats zal vinden geen beslissing van de onderzoekers is.
Tabblad DPIA, vrg 5	Licht toe welke data met de OSIRIS data wordt bedoeld Er is verder toegelicht wat de OSIRIS data zijn en waarom die voor het onderzoek nodig zijn
Tabblad DPIA, vrg 6	Geef aan dat niet alleen BSN en geboortedatum worden verwijderd maar ook naw, tel.nr. en e-mailadres (zie vrg. 57) Dit is toegevoegd. Omdat sinds het datalek bij GGD GHOR NL BSN niet meer een te downloaden item kan deze niet in onze data terechtkomen. We hebben elke verwijzing naar BSN verwijderd in deze DPIA.
Tabblad DPIA vrg 6	Geef aan welke personen als onderzoeker toegang kunnen krijgen tot de data. Geef aan hoe deze toegang zich verhoudt tot 5. in het Tabblad doelen + verwerkingen. Hier staat dat de analyses centraal worden gedaan door onderzoekers van GGD Amsterdam Onderzoekers zijn personen die toestemming hebben gekregen van de CONTROL stuurgroep om CONTROL data in de cloud in te zien en te analyseren.
Tabblad 'DPIA', vrg 6	Geef aan welke gegevens worden bedoeld, bijv. de OSIRIS data? Licht toe op welke wijze sprake zou kunnen zijn van discriminatie/stigmatisering/uitsluiting Toevoegen: kans op een datalek Er is toegelicht om welke gegevens het gaat en hoe die mogelijk aanleiding zouden kunnen geven tot stigmatisering etc. Daarnaast is aangegeven dat een datalek nooit 100% uitgesloten kan worden, en het risico op stigmatisering dan zal stijgen.
Tabblad 'Risico's en maatregelen' Niet geautoriseerde personen krijgen toegang tot de data in de DRE	1. 1x per kwartaal wordt de logging gecheckt. Dit is maar 4x per jaar. Geef aan waarom dit voldoende is 2. Zijn medewerkers geïnformeerd over het checken van de logging? Is de OR geconsulteerd? 3. Door wie en hoe vaak worden autorisaties gecheckt? Toegang tot de cloud kan enkel verkregen worden wanneer een persoon actief is aangemeld voor de service door de projectleider of de data steward. Wanneer een gebruiker data wil verwijderen of downloaden wordt er direct een email verstuurd aan de projectleider en de data steward die deze moeten actief moeten goedkeuren voordat het kan worden uitgevoerd. Dit wordt dus continu gemonitord. Minder frequentie monitoring van het inloggen kan, omdat de data die grotendeels gecodeerd zijn en dus niet geïnterpreteerd kunnen worden, is vanuit beveiliging voldoende. De projectleider rapporteert inlogbevindingen aan de stuurgroep. De medewerkers zijn op de hoogte van de logging. Zij tekenen een gebruikersovereenkomst waarin dit is gemeld
Tabblad 'Risico's en maatregelen' Informerende van betrokkenen	Geef aan waarom burgers niet worden geïnformeerd bij het aanmelden / uitvoeren van de test. Niet goed informeren van betrokkenen is een serieus risico. Zeker gezien de reputatieschade voor de GGD als gevolg van het recente datalek. Communicatie aan betrokkenen dient goed te zijn ingeregeld alvorens met het onderzoek wordt gestart. De burger meldt zich aan bij GGD GHOR NL voor een coronatest in een van de teststraten. Het ligt niet binnen de mogelijkheden van CONTROL om informatie te verspreiden aan de Betrokkene(n) via GGD GHOR NL. Wij hebben zelf geen direct contact met de burgers. We gebruiken retrospectief verzamelde gegevens vanaf 1 juni 2020. In de privacyverklaring van de GGD Amsterdam wordt melding gemaakt van het doen van wetenschappelijk onderzoek op routine data.

Tabblad 'Risico's en maatregelen'	Geef aan hoe stigmatisering wordt voorkomen. Momenteel is onduidelijk hoe wordt voorkomen dat bepaalde groepen onnodig en onterecht worden gestigmatiseerd. Zowel privacy risico voor betrokkenen als reputatierisico voor de GGD. Zie ook eerdere opmerkingen over gebruik geboorteland, beroep en religie.
Profilering	Dit punt is samengevoegd met het risico 'De onderzoeksresultaten kunnen aanleiding geven tot discriminatie van bevolkingsgroepen'. Er is hierin verder toegelicht hoe de resultaten gebruikt worden en hoe daarin het risico op stigmatisering zoveel mogelijk beperkt wordt.

DPIA visie 5.1.2e VGGM	
Algemeen	De DPIA is zeer zorgvuldig uitgevoerd waarbij er voldoende oog is voor de rechten en vrijheden van betrokkenen. De DPIA laat zien dat aan het verwerken van de persoonsgegevens risico's kleven, maar dat er voldoende maatregelen genomen worden om de risico's die het onderzoek meebrengt, te mitigeren door middel van het nemen van technische en organisatorische maatregelen. Als 5.1.2e VGGM ben ik dan ook van mening dat het restrisico kan worden geaccepteerd op voorwaarde dat de voorgestelde maatregelen en verbeteringsuggesties worden overgenomen welke in deze DPIA zijn beschreven. Daarnaast is onderstaand advies op specifieke punten toegevoegd. Deze dienen nader uitgewerkt te worden.
Informerende van betrokkene	Op basis van deze referentie DPIA kan worden gesteld dat transparante communicatie naar betrokkenen als belangrijk wordt gezien. Hiervoor is een privacy statement opgesteld https://www.ggd.amsterdam.nl/beleid-onderzoek/projecten/control-privacy/. Het privacy statement dient door de eigen GGD beschikbaar gemaakt te worden op de website of te verwijzen naar het statement van GGD Amsterdam.
Grondslag en beperking	Art 24 UAVG legt de basis om het onderzoek te kunnen starten. Op basis van dit artikel en art. 89 AVG worden echter ook de voorwaarden meegegeven waaraan het onderzoek moet voldoen. Hiertoe wordt ook pseudonimisering gerekend. Het is mij echter onduidelijk of alle variabelen voor het onderzoek benodigd zijn. Hoe meer variabelen, hoe meer dit zegt over de persoon en mogelijke herleidbaarheid.

Bijlage 4b

BIV Amsterdam

BIV Classificatie gegevensstroom

Beschikbaarheid

Gevolgen van het niet beschikbaar zijn van informatie (in een systeem of document)

[illegible]

Integriteit					
Gevolgen van foute -onjuiste en/of onvolledige- informatie (in het ergste geval)					
omschrijving waarde	omschrijving waarden integriteit				
0 - Niet zeker	De informatie mag worden veranderd. Geen extra bescherming van integriteit is noodzakelijk. Schending van integriteit heeft geen gevolgschade.				
1 - Beschermd	Het proces dat gebruik maakt van deze informatie staat enkele (integriteits-)fouten toe. Een basisniveau van beveiliging is noodzakelijk. Schending van integriteit kan enige (in-)directe schade toebrengen.				
2 - Hoog	Het proces dat gebruik maakt van deze informatie staat zeer weinig (integriteits-)fouten toe. Bescherming van integriteit is absoluut noodzakelijk. Schending van integriteit kan serieuze (in)directe schade toebrengen. Ernstige schade: krantenkoppen, vragen van belangrijke partners/klanten, burgers, budgettaire problemen.				
3 - Absoluut	Het proces dat gebruik maakt van deze informatie staat geen (integriteits-)fouten toe. Schending van integriteit kan (zeer) grote schade toebrengen. Zeer ernstige schade: raadsragen, kamervragen, reactie minister of wethouder vereist, belangrijke partners/klanten stellen professionaliteit van het rijk of de gemeentelijke dienst ter discussie.				
		<u>Waardering (selecteer een waarde)</u>			
		<u>Argumentatie (verplicht invullen)</u>			
	11 Managementbeslissingen: hoe schadelijk is het als op basis van foute (onjuiste en/of onvolledige) informatie verkeerde managementbeslissingen worden genomen?	0			Management beslissingen worden niet genomen obv deze data/analyses
	12 Fraude: welke gevolgen heeft foute informatie op het risico van fraude/ fraudulueze handelingen	3			Data manipulatie/fraude in de wetenschap geeft imagoschade
	13 Onderbreking van het proces: in hoeverre wordt het proces onderbroken als gevolg van foute (onjuiste en/of onvolledige) informatie?	0			Bij fouten kan het proces door en kunnen we opnieuw de brondata aanvragen
	14 Vertrouwen van het publiek of burgers/ patiënten: in hoeverre kan het vertrouwen van het publiek of gebruikers/patiënten worden geschaad door foute (onjuiste en/of onvolledige) informatie?	2			Imagoschade vanwege fraude in wetenschap en bij GGD
	15 Wettelijke aansprakelijkheid: wat zijn de gevolgen van het niet voldoen aan wettelijke of contractuele verplichtingen die veroorzaakt worden door foute informatie?	0			Wettelijke verplichtingen zijn nvt
	16 Additionele kosten: in hoeverre kunnen additionele kosten ontstaan door foute informatie? Bijvoorbeeld door het moeten herstellen van een corrupte database of opnieuw invoeren van gegevens.	1			Personele kosten van nieuwe dataextractie, upload en analyse
	17 Moreel van de medewerkers: wat zijn de gevolgen op het moreel van medewerkers als foute informatie wordt verwerkt?	0			De groep medewerkers is heel klein
Wat is de meest serieuze impact als informatie onjuist/ onvolledig is?		3			Waarde wordt automatisch berekend
BIV- classificatie integriteit		3 - Absoluut			Waarde wordt automatisch berekend

Vertrouwelijkheid					
Gevolgen van ongeautoriseerde verspreiding van informatie (in het ergste geval)					
<u>Omschrijving waarde</u>	<u>Omschrijving waarden vertrouwelijkheid</u>				
0 - Openbaar	Alle informatie die algemeen toegankelijk is voor iedereen. Er is geen schending van vertrouwelijkheid mogelijk en sprake van verwaarloosbare schade of niet van toepassing.				
1- Bedrijfsvertrouwelijk	Informatie die toegankelijk mag of moet zijn voor alle medewerkers van de eigen organisatie(s). Vertrouwelijkheid is gering. Schending van vertrouwelijkheid kan enige (indirecte) schade toebrengen. Acceptabele schade binnen marges; incident met direct betrokkenen is (snel) recht te zetten.				
2 - Vertrouwelijk	Informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers. De informatie wordt ter beschikking gesteld op basis van vertrouwen. Schending van vertrouwelijkheid kan serieuze (indirecte) schade toebrengen. Ernstige schade: klantenkoppen, vragen van belangrijke ketenpartners, politiek, burgers en afnemers.				
3 - Geheim	Dit betreft gevoelige informatie die alleen toegankelijk mag zijn voor de direct geadresseerde. Schending van vertrouwelijkheid kan zeer grote schade toebrengen. Zeer ernstige schade: raadvragen, reactie wethouder vereist, belangrijke ketenpartners / klanten stellen professionaliteit van de gemeentelijke dienst ter discussie.				
			<u>Waardering (selecteer een waarde)</u>	<u>Argumentatie (verplicht invullen)</u>	
V1	Vertrouwen van de burger/patient: wat zijn de gevolgen voor de GGD indien informatie te vroeg c.q. niet volgens de regels wordt verspreid?	3		(Weer) een datalek levert grote imago-schade op. Data zijn gecodeerd en gepseudonimiseerd, dus werkelijke schade voor de burger is klein omdat kans op herleidbaarheid klein is.	
V2	Vertrouwen van het publiek: wat zijn de gevolgen voor het publieke imago van de GGD als informatie van de organisatie onterecht wordt verspreid?	3		Er is al een datalek geweest bij GGD GHOR NL. Nu kunnen binnen het CONTROL project geen direct herleidbare gegevens lekken, want die hebben we niet. Daarmee is een eventueel werkelijk impact van een lek minder ernstig. Qua beeldvorming is het wel ernstig.	
V3	Ketensamenwerking: kan de GGD toegang tot de keten in het proces geweigerd worden?	0		proces is wetenschappelijk onderzoek geïnitieerd door de GGD zelf	
V4	Vertrouwen van ketenpartners: wat zijn de gevolgen voor de relatie met de ketenpartners van de GGD, als informatie onterecht wordt verspreid?	2		in het project werken we samen met 7 andere GGD'en en het RIVM die ons hun gepseudonimiseerde data toevertrouwen. Werken op andrea hebben we als GGD Amsterdam voorgesteld, maar de beslissing dit te doen is gezamenlijk besloten en opgenomen in de verwerkersovereenkomst	
V5	(Wettelijke) Aansprakelijkheid: wat zijn de gevolgen voor (wettelijke) aansprakelijkheid bij het onterecht verspreiden van informatie?	2		GGD is aansprakelijk in geval van lek, maar schade voor burger is beperkt (gezien moeilijke herleidbaarheid)	
V6	Additionele kosten: in hoeverre is sprake van additionele kosten door onterechte verspreiding van informatie?	0		mogelijk wat personele kosten voor rectificatie	
V7	Moreel van de medewerkers: in hoeverre kan een duidelijk negatieve invloed op het moreel en de motivatie van medewerkers een gevolg zijn van de onterechte verspreiding van informatie?	0		de groep die met deze data werkt is heel klein en het moreel is al aangetast door het recente GGD NL datalek	
Wat is de meest serieuze impact als informatie ongeautoriseerd wordt verspreid?		3		Waarde wordt automatisch berekend	
BIV- classificatie vertrouwelijkheid		3 - Geheim			

5.1.2e

GGD Amsterdam

Eindadvies Informatiebeveiliging			
De scores op de verschillende aspecten van de BIV-vragen (Beschikbaarheid, Integriteit en Vertrouwelijkheid) wijzen uit:			
• Het aspect Beschikbaarheid (1) geen verhoogd risico kent; • Het aspect Integriteit (3) een verhoogd risico kent; • Het aspect Vertrouwelijkheid (3) een verhoogd risico kent.			
Dat betekent dat de maatregelen uit:			
1. De NEN7510;			
2. de SaaS-maatregelen van gemeente Amsterdam (zie bijlage mail);			
3. de onderstaande BIV-tabellen aan maatregelen nodig zijn de beveiliging van het informatiesysteem.			
</			

	Integriteit	
	Niveau "Absoluut" (0 rating: 3):	
	Authenticatie 'hoog' vereist	Midden (2 factor): authenticatie gebaseerd op iets wat men weet en iets wat men heeft (bijv. een token, smartcard of certificaat)
	Identificatie personen	Persoonlijk (Named)
	Identificatie systemen	Groep / Uniek
	Authenticatie personen	Kennis (wachtwoord) + Bezit (Token / Certificaat) + Fijnschap (iiscan/vingerafdruk)
	Authenticatie systemen	*Client: Certificaat Server: Certificaat
	Authenticatie beleid	Veilig geachte Hash + certificaat authenticiteit
	Autorisatie toekenning	Autorisatie vereist d.m.v. 4 ogen principe
	Autorisatie beleid	Toegangscontrole centraal (centrale directory)
	Autorisatie model	RBAC
	Autorisatie voor beheerders directe toegang data	Functioneel beheer: Integriteitsverklaring Technisch beheer: Geen toegang Hosting beheer: Geen toegang Infra beheer: Geen toegang
	Beheer en data verkeer logisch gescheiden	Ja
	Systeem autorisatie	Leveranciers: Onder begeleiding Functioneel beheer: Integriteitsverklaring Technisch beheer: Integriteitsverklaring Hosting beheer: Integriteitsverklaring Infra beheer: n.v.t.
	Systeem verhoogde rechten	Leveranciers: Nee Functioneel beheer: Nee Technisch beheer: Nee Hosting beheer: Ja Infra beheer: n.v.t.
	Soort log	Authenticatie + Input/Output + Data
	Herleidbaarheid data (logging)	Geen
	Herleidbaarheid authenticatie (logging)	Wie + waartmee/- wanneer + wat + resultaat
	Herleidbaarheid transport (logging)	Wie + wanneer + wat + transport nummer + resultaat
	Bewaar termijn logs	3 jaar of langer
	Bewaren (herleidbare) persoonsgegevens > 6 maanden	Melding gedaan worden bij 5.1.2e
	Activiteiten n.a.v. logs	Proactief: Automatische detectie met manuele runbooks
	Tijdynchronisatie	Ja, minimaal stratum 3
	Beheer toegang tot logs	Nee
	Opslag van logs	Centraal
	Toegang tot logs	Identificatie + leesrechten
	Invoervalidatie	Ja
	(Malafide code detectie / Virus / Trojan / Spam)	
	Controle op mutaties tijdens transport	Ja
	Data transport beveiliging	Transport beveiliging + berichtbeveiliging / bestandbeveiliging
	Gegevens kenmerk	Gegevens worden niet buiten hun bron opgeslagen (behalve voor beschikbaarheid) en niet buiten hun bron gewijzigd.
	Gegevens consistentie borging	Ja
	Patch beleid	Patches worden actief gemonitord en beoordeeld en in overleg met de leveranciers toegepast

Vertrouwelijk		
Niveau "Geheim" (V rating: 3):		
Hardening	Locatie + Hardware + Netwerk + Systeem + Middleware + Software	
Authenticatie personen / deblokkering	Kennis (wachtwoord) + Bezit (Token / Certificaat)	
Authenticatie systemen	Client: Certificaat	
	Server: Certificaat	
Autorisatie vereiste	Specifiek: Specifieke rol	
Sessie kenmerk	Sessie timeout na 15 minuten inactiviteit	
	Sessie timeout voor klanten na 120 minuten absoluut	
	Identiteit: blokkering na 3 achtereenvolgende foutieve authenticatie pogingen	
	Single Sign On niet toegestaan	
Herleidbaarheid authenticatie (logging)	Wie + waar(mee) + wanneer + wat + resultaat	
Bewaar termijn logs	7 jaar of langer	Bewaartermijn persoonsgegevens is max 3 mnd na beëindiging CONTROL. Dit hanteren we ook voor logs. Tussentijdse monitoring maakt langere bewaartermijn onnodig.
Code uitvoering validatie (o.a. SQL injectie)	Ja	
Data kopiëren / transport	Geen kopiëren behalve voor beschikbaarheid en alleen transport binnen het vaste netwerk van gemeente Amsterdam (gemeentelijke zone)	
Productie data voor OTA	Niet toegestaan, tenzij de data is geanonimiseerd en toestemming is van de geveenseigena(r)en	
Back-end netwerk delen toegestaan met	Alleen voor gebruikers (Geïsoleerd)	
Hardware virtueel delen toegestaan met	Alleen voor gebruikers (Geïsoleerd)	
Scheiding applicaties	Individueel	
Scheiding applicaties van data	Netwerk	
Scheiding OTAP	Netwerk	
Data opslag bescherming	Toegangscontrole + encryptie	
Backup opslag bescherming	Toegangscontrole voor technisch beheer + encryptie	
Transport data binnen de systeemoplossing (PAN)	Berichtbeveiliging / bestandbeveiliging	
Transport data binnen datacenter (LAN)	Berichtbeveiliging / bestandbeveiliging (met certificaat autoriteit)	
Transport over vertrouwde netwerken (MAN)	Transport beveiliging en berichtbeveiliging / bestandbeveiliging (met certificaat autoriteit)	
Transport over externe netwerken (WAN)	Transport beveiliging en berichtbeveiliging / bestandbeveiliging (met certificaat autoriteit)	
Functionele scheiding	Mandaat / gebruik / functioneel beheer / technisch beheer	
Host firewall	Ja	
Indringers detectie systeem	IPS + IDS	
Afvoeren datadragers	Beveiligde vernietiging van data dragers	

5.1.2e

GGD Rotterdam-Rijnmond

RE: CONTROL Verwerkersovereenkomst & DPIA



5.1.2e

Aan 5.1.2e 5.1.2e 5.1.2e
CC 5.1.2e 5.1.2e 5.1.2e

 Dit bericht maakt deel uit van een gevolgd gesprek. Klik hier als u alle verwante berichten wilt vinden of het oorspronkelijke bericht met vlag wilt openen.

Ho! 5.1.2e en 5.1.2e

Ik heb de bijlage 3 bekeken. Het ziet er gestructureerd uit.

- Op het tabblad BIA staat een BIV-classificatie

- N.a.v. deze BIV-classificatie staat op het tabblad Advies 5.1.2e ongeveer 100 maatregelen aanbevolen op basis van NEN7510

- Ik mis nog een aanvullende Risico Impact Analyse waarmee mogelijke onvoorziene risico worden opgepakt.

- Voor de Procedure externe verbindingen zijn de Saas-maatregelen van toepassing

In deze adviezen is de **Opzet** besproken, over het **Bestaan** en de **Werking** kan ik niks zeggen.

In zijn algemeenheid zie ik dat binnen de GGD-en en GGD GHOR met NEN7510 wordt gewerkt, wij werken met de BIO. Komt in essentie op hetzelfde neer, ze zijn beide op ISO27001 gebaseerd. De BIO is wel uitgebreider en completer.

Met vriendelijke groot,

5.1.2e

Gemeente Rotterdam
Bestuurs- en concernerondersteuning
Afdeling Informatiemanagement
IM MOIV&I
Schiedamsedijk 95
Postbus 70032-3000 LP Rotterdam
Mobiel 5.1.2e
Website www.rotterdam.nl

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst, Bijlage 5

Bijlage 5 Variabelen lijst

Laatste update: 23-06-2021

Inhoudsopgave

Notities vooraf	2
Variabelen uit CoronIT	3
Variabelen uit HPZone – Cases/contacten	7
Variabelen uit HPZone – Situations	12
Variabelen uit HPZone – Contexten	13
Variabelen uit HPZone – Actions	14
Variabelen uit HPZone – Monitoring calls	15
Variabelen uit HPZone – Investigations	16
Variabelen uit HPZone – Case/situation link table	17
Variabelen uit HPZone – Case/contact link table	17
Osiris Variabelen	18

Notities vooraf

In dit document zijn de variabelen beschreven die voor CONTROL worden geëxtraheerd. Er is een beschrijving van de variabele toegevoegd, of het een persoonsgegeven betreft, wat de reden is voor gebruik en wanneer er codering of een hash wordt toegepast.

CONTROL gebruikt data gerelateerd aan SARS-CoV-2 testen en bron- en contactonderzoek uit de periode 1 juni 2020 tot 1 maart 2021. Sommige Partijen gebruiken HPZone ook voor andere andere infectieziekten. Bij sommige downloads uit HPZone kan niet geselecteerd worden op periode of infectie. Data die niet binnen de scope van CONTROL vallen, maar wel in de HPZone downloads zijn meegekomen worden zoveel mogelijk verwijderd door het R script. Het advies aan de data managers is om te controleren of de set die wordt klaargezet voor uploaden ook alleen records bevat die gebruikt worden in dit project.

Omdat bekend is dat de GGD'en HPZone niet allemaal op eenzelfde manier gebruiken en het voor kan komen dat vergelijkbare gegevens in andere velden wordt opgeslagen vindt er na uploaden van alle data een check plaats hoe de data zijn ingevuld en welke variabelen alsnog worden verwijderd uit de data. Interpretatie van variabelen gebeurt in overleg met de Partij van wie de data afkomstig zijn. Na deze harmonisatie stap volgt een nieuwe Variabelen lijst met de definitieve variabelen die CONTROL opslaat voor analyse. Die lijst wordt gecirculeerd in de stuurgroep en de werkgroep.

Variabelen uit CoronIT

Variabele naam	Type	Values & value labels	Beschrijving	(Bijzonder) persoons gegeven ja/nee	Reden gebruik	Codering
Afnamelocatie	String	Naam van de teststraat waar de test is uitgevoerd	Testlocatie	Nee	Mogelijke determinant van doorlooptijd corona test/bco keten	
Afnumerimte	String	Naam/identificatie van locatie in de teststraat waar de test is uitgevoerd	Gedetailleerdere beschrijving van de testlocatie (bijv. welke tent of fiets/auto)	Nee	Mogelijke determinant van doorlooptijd corona test/bco keten	
Afspraak.aangemaakt	Datetime		Datum/tijd waarop de testafspraken is gemaakt	Nee	Doorlooptijd indicator	
Afspraak.afgerond	Datetime		Datum/tijd waarop de afspraak is afgerond (uitslag bekend)	Nee	Doorlooptijd indicator	
Afspraak.start	Datetime		Datum/tijd waarop de afspraak is gestart (moment waarop cliënt zou moeten verschijnen op de testlocatie)	Nee	Doorlooptijd indicator	
Afspraak_aangemaakt_door	String	"Portaal" = afspraak gemaakt via online portaal Naam medewerker = afspraak is niet via online portaal gemaakt, maar per telefoon	Hoe is de testafspraken aangemaakt?	Ja	Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO	"Portaal" of "Telefoon" (wanneer naam in het veld staat, als anonimiseren)
Afspraak_status	String	Vervallen/ Afgerond/ Gepland/ Geannuleerd	Wat is de status van de afspraak?	Nee	Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO	

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst, Bijlage 5

Datum.monsterafname	Datetime		Datum waarop het testmateriaal is afgenomen bij de cliënt in de teststraat	Nee	Doorlooptijd indicator	
Datum.uitslag	Datetime		Datum waarop de testuitslag is ingevoerd in CoronIT	Nee	Doorlooptijd indicator	
Deelname_status	String	Aanwezig/ Afgezegd/ Geannuleerd/ Gepland/ Geweest/ No show	Wat is de status van de afspraak? (verschil met afspraak status onduidelijk)	Nee	Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO	
Gemeente	String		In welke gemeente woont de cliënt	Nee		
Geslacht	String	Man/ Vrouw/ Onbekend/ Niet_gespecificeerd	Van welk geslacht is de cliënt?	Ja	Nodig voor koppeling CoronIT/HPZone. Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO	Hash + salt
GGD_testlocatie	String	Naam GGD	GGD waar de test is uitgevoerd	Nee	Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO & mogelijke indicator van obstakels in de corona test/bco keten	
GGD_werkgebied	String	Naam GGD	Onder welke GGD valt de patiënt	Nee	Mogelijke indicator van obstakels in de corona test/bco keten	
Laboratorium_naam	String	Naam laboratorium	Laboratorium waar de SARS-CoV-2 test is uitgevoerd	Nee	Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO	
Land	String	Naam land	Waar woont iemand	Ja	Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO	Hash + salt
Naam_gebruik		Eigen/ Partner/ Eigen_partner/ Partner_eigen	Is afspraak gemaakt door client zelf of door partner?	Nee	Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO	

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst, Bijlage 5

Plaats	String	Naam woonplaats	Woonplaats cliënt	Nee	Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO	
Postcode	String	6 digits postcode	Postcode woonadres cliënt	Ja	Nodig voor de koppeling met HPZone. Na koppelen wordt deze omgezet naar postcode-4. Dit is een mogelijke determinant van doorlooptijd corona test/bco keten (afstand tot teststraat als barriere) & effectiviteit BCO (SES indicatoren buurt)	Postcode-4
Uitslag	String	Negatief/Positief/ Onbekend/ Onbeoordeelbaar		Ja	Medisch gegeven. Indien positief, dan wordt een BCO uitgevoerd. De doorlooptijd vanaf het ontstaan van klachten beïnvloedt de effectiviteit van het BCO. Onderzoek wordt gedaan naar vertraging die optreden door onbeoordeelbare uitslagen	0 = Negatief 1 = Positief 2 = Onbekend 3 = Onbeoordeelbaar
uitslag_via_portaal	String	Onwaar/ Waar	Is de testuitslag via het online portaal opgevraagd? [twijfel over betekenis]	Nee	Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO	
hash_patient_nr	String		Client identifier	Ja	Nodig voor koppeling CoronIT/HPZone en/of structuur in de data	MD5 Hash + Salt
hash_sample_nr	String		Bezoek/sample identifier			
hash_pers_identifier	String		Hash van achternaam + pc6 + geboorteland + salt			
leeftijd_jaren	Int		Leeftijd in jaren, afgeleid van geboortedatum	Ja	Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO	

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst, Bijlage 5

BCO_nummer	Int		BCO identifier van contact in het geval dat ze via BCO zijn doorverwezen	Ja	Nodig voor koppeling CoronIT/HPZone en/of structuur in de data	
Bijzondere_doelgroep	String	BCO/ Patiënt / Risicogroep	Tot welke bijzondere doelgroep behoort de cliënt?	Ja	Mogelijke determinant in BCO prioritering	
Beroepsgroep_type_zorgverlener	String	Thuiszorg, tandarts, huisarts, zkh, etc.	Case waaraan gerelateerd als BCO	Ja	Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO	
Beroepsgroep_contactberoep	String	Winkelmedewerker, kapper, pedicure etc.	Beroep als het in een van de categorieën valt			
Notificatie_coronamelder	String	Ja/nee/weet niet	Heeft de client een coronamelder melding ontvangen?	Nee	Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO	
Aantal_klachten	Int			Ja	Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO	
Klachten	String	Lijst {} met klachten (hoesten, smaakverlies, reukverlies, koorts, neusverkouden, benauwdheid, keelpijn, spierijn, geen van deze)	Welke zelf-gerapporteerde klachten heeft de cliënt ten tijde van de test aanmelding?			

Variabelen uit HPZone – Cases/contacten

Variabele	Type	Values & value labels	Beschrijving	(Bijzonder) persoons gegeven ja/nee	Reden gebruik	Codering
Locality	String		Gemeente waar de cliënt woont	Nee	Mogelijke determinant van doorlooptijd & effectiviteit BCO	
Town	String		Stad/dorp waar de cliënt woont	Nee	Mogelijke determinant van doorlooptijd & effectiviteit BCO	
Type	String	Case/contact	Karakterisering van record als record van een case of contact	Ja	Selectievariabele, cluster informatie. Mogelijke determinant van doorlooptijd & effectiviteit BCO	
Diagnosis	String	COVID-19	Diagnose SARS-CoV-2 infectie	Ja	Selectievariabele. Mogelijke determinant van doorlooptijd & effectiviteit BCO	1 = COVID-19
Confidence	String	Confirmed/discarded/possible/probable	Zekerheid van de diagnose			
Priority	String	Amber / green / red	Prioriteit indicator van het BCO	Ja	Mogelijke determinant van doorlooptijd & effectiviteit BCO	
Status	String	Open / closed	Huidige status van het BCO	Nee	Doorlooptijd indicator	
Date closed	Datetime		Datum dat het dossier is afgesloten		Doorlooptijd indicator	
Date of Onset	Datetime		Datum start symptomen	Ja	Doorlooptijd indicator Mogelijke determinant van doorlooptijd & effectiviteit BCO	
Date of Onset Resolution	String	Bekend / geschat / asymptomatisch	Beschrijving van EZD, zeker, geschat, asympt.	Ja	Doorlooptijd indicator	

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst, Bijlage 5

					Mogelijke determinant van doorlooptijd & effectiviteit BCO	
Current Location	String		Huidige verblijfslocatie	Ja	Mogelijke determinant van doorlooptijd & effectiviteit BCO	
Recent travel to another country	String	Naam land	In welk land is de cliënt recent geweest? Indien van toepassing [definitie recent onbekend]	Ja	Mogelijke determinant van doorlooptijd & effectiviteit BCO	
Principal Contextual Setting	String	Naam van de setting	Belangrijkste setting waar de cliënt is geweest in de periode dat de cliënt geïnfecteerd raakte. Meestal de meest waarschijnlijke bron van infectie	Ja	Mogelijke determinant van doorlooptijd & effectiviteit BCO	
Hospitalised	String	Yes/no/not known	Is de cliënt opgenomen in het ziekenhuis?	Ja	Medisch gegeven, Mogelijke determinant van doorlooptijd & effectiviteit BCO	
Diagnostic Notes	Text		Notities bij de case (samenvatting e.d.)	Ja, mogelijk	Diverse informatie over de cliënt die door de BCO medewerker als relevant werd gezien voor de verspreiding van het virus en bevat mogelijk determinanten van doorlooptijd & effectiviteit BCO & verspreidingspotentieel	Relevante data worden geautomatiseerd met woordherkenningstechnieken uit dit veld gehaald waarna dit veld uit de data wordt verwijderd
Date of death (where appropriate)	Datetime	Datum indien overleden en datum bekend	Wanneer is de cliënt overleden?		Mogelijke determinant van doorlooptijd & effectiviteit BCO & verspreidingspotentieel	

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst, Bijlage 5

		Leeg indien niet overleden of onbekend				
Case Manager_Id	String		Medewerker die cases verdeelt over BCO'ers	Ja	Selectie variabelen voor in-/exclusie records in analyse en relevant voor scoring uitvoer kwaliteit BCO.	MD5 hash + salt
Investigating Officer_Id	String		Medewerker die BCO uitvoert			
Entered by_Id	String		Medewerker die case heft ingevoerd (als niet via CoronIT is gepusht)			
Time entered	Datetime		Wanneer is record aan HPZone toegevoegd	Nee	Doorlooptijd indicator Mogelijke determinant van doorlooptijd & effectiviteit BCO	
Municipality	String		Gemeente client	Nee	Mogelijke determinant van doorlooptijd & effectiviteit BCO	
Import Source	String	Leeg of coronit	Is de case via CoronIT in HPZone gekomen of niet? Leeg voor contacten	Nee	Doorlooptijd indicator Mogelijke determinant van doorlooptijd & effectiviteit BCO	
Probable Transmission Route	String	Aerogeen / mens op mens/ onbekend	Meest waarschijnlijke route van transmissie	Nee		
Relationship to the above case	String		Relatie tot index case	Ja	Cluster informatie. Mogelijke determinant van doorlooptijd & effectiviteit BCO	
Degree of Contact	String	Cat 1, 2 of 3	Type contact			
Additional comments on the nature of the contact with Index Case	String		Notities contact			
Pregnant	Bool	Yes/No	Zwanger ja/nee	Ja	Mogelijke determinant van doorlooptijd & effectiviteit BCO Kunnen van invloed zijn op de prioriteit die	
Newborn	Bool	Yes/No	Pasboren baby ja/nee			
Hartaandoening	Bool	Yes/No	Hartaandoening ja/nee			
Leveraandoening	Bool	Yes/No	Leveraandoening ja/nee			
Nieraandoening	Bool	Yes/No	Nieraandoening ja/nee			

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst, Bijlage 5

Luchtwegaandoening	Bool	Yes/No	Luchtwegaandoening ja/nee		gegeven wordt aan het BCO, het contactnetwerk waar iemand in zit en de mogelijkheid tot meewerken aan het BCO	
Diabetes Mellitus	Bool	Yes/No	Diabetes Mellitus ja/nee			
Immuungecompromitteerd	Bool	Yes/No	Immuungecompromitteerd ja/nee			
Maligniteit	Bool	Yes/No	Maligniteit ja/nee			
Anders	Bool	Yes/No	Andere aandoening?			
Intravenous Drug User	Bool	Yes/No	Injecterend drugsgebruik ja/nee?			
Works with Food	Bool	Yes/No	Werkzaam in de voedselindustrie ja/nee?	Ja	Mogelijke determinant van doorlooptijd & effectiviteit BCO Bepalend voor aantal contacten en prioritering BCO en dus voor de effectiviteit	
Works in Health Care	Bool	Yes/No	Werkzaam in de gezondheidszorg ja/nee?			
Works in Education	Bool	Yes/No	Werkzaam in het onderwijs ja/nee?			
Indicate other risk factors	Bool	Yes/No	Andere risicofactoren ja/nee?			
Details of other special risk factors surrounding this case	String		Indien Details over andere risicofactoren, indien other risk factors is ja			
Vaccinated in respect to the diagnosis	String	Ja/nee / onbekend	Is de cliënt gevaccineerd tegen SARS-CoV-2?	Ja	Bepaald verspreidingspotentieel en beïnvloedt mogelijk het aantal contacten	
Vaccination Date (if relevant)	Datetime		Wanneer is de client gevaccineerd tegen SARS-CoV-2?			
Oorspronkelijke bron van de melding	String	Lab / GGD/ werkgever etc.				
Aanvullende informatie over de melder	String	Externe partij bijv.	Extra details over de melder die de infectie heeft gemeld aan GGD. Melder kan commerciële partij, instelling, cliënt, etc zijn.			
Laboratorium waar de casus gediagnosticeerd is	String		Naam laboratorium waar de SARS-CoV-2 test is			

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst, Bijlage 5

			uitgevoerd (ook wanneer test via andere route dan CoronIT is uitgevoerd)			
GP Practice die de casus gediagnosticeerd heeft	String		Naam huisarts(en praktijk) die de diagnose heeft gesteld (indien van toepassing)	Ja	Medisch gegeven. Mogelijke determinant van doorlooptijd	Anonimisering dmv codering huisarts ja/hee
Datum melding aan de GGD	Datetime		Datum waarop de case die elders is gediagnosticeerd is gemeld bij de GGD	Nee	Doorlooptijd indicator	
Datum gefiatteerd in Osiris	Datetime		Datum waarop eerste record vragenlijst is aangemaakt			
Datum definitief in Osiris	Datetime		Datum waarop vragenlijst naar OSIRIS is verstuurd			
Status van de melding	String	Gefiatteerd/definitief			Procesanalyse BCO	
Datum gewist	Datetime		Datum dat de casus gewist is		Kwaliteitsindicator	
Gender	String		Van welk geslacht is de cliënt?	Ja	Nodig voor koppeling CoronIT/HPZone. Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO	Hash
country_birth_hash	String		Geboorteland van de cliënt	Ja		
Leeftijd_jaren	Int			Ja	Nodig voor koppeling CoronIT/HPZone. Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO.	
hash_pers_identificer	String		Identificer voor linken records tussen CoronIT en HPZone	Ja	Nodig voor koppeling CoronIT/HPZone	Hash

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst, Bijlage 5

hash_case_identifier	String		Record identifier voor linken diverse tabellen in HPZone	Ja	Nodig voor behoud data structuur	Hash
hash_contact_of	String		Identifier voor het linken van cases en contacten	Ja		Hash

Variabelen uit HPZone – Situations

Variabele	Type	Values & value labels	Beschrijving	(Bijzonder) persoons gegeven ja/nee	Reden gebruik
Unique Identifier	String		Record identifier	Nee	Nodig voor behoud data structuur
Type	String	Cluster/outbreak	Type situation	Nee	Cluster informatie.
Name	String		Situation identifier	Nee	Cluster informatie. Mogelijke determinant van effectiviteit BCO.
Title	String		Titel van de situation	Nee	Cluster informatie.
Risk Level	Int	Level 1/ level2	Risico van de situation	Nee	Mogelijke determinant van effectiviteit en prioritering BCO.
Start Date	Datetime		Start datum situation	Nee	Cluster informatie.
Location	String		Locatie van de situation	Nee	Cluster informatie.
Gemeld in Osiris	String	Yes/No	Wel of niet gemeld Osiris	Nee	Koppelvariabele en prioriteringsvariabele
Identification Number (Internal)	Int		Id nummer situation	Nee	Cluster informatie.
Manager_Id	String		Situation manager id (gehasht)	Ja	Koppelvariabele nodig voor behoud data structuur
Severity	Int	0,1,2,3,4	Severity van situation	Nee	Mogelijke determinant van effectiviteit en prioritering BCO.

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst, Bijlage 5

Intervention	Int	0,1,2,3,4	Maatregelen situatie	Nee	Mogelijke determinant van effectiviteit en prioritering BCO.
Brief Description	String		Omschrijving van de situatie en beoordeling	Nee	Mogelijke determinant van effectiviteit en prioritering BCO.

Variabelen uit HPZone – Contexten

Variabele	Type	Uitleg	(Bijzonder) persoonsgeven ja/nee	Reden gebruik
Context.Identifier	String	Record identifier	Nee	Nodig voor behoud data structuur
Context	String	Naam / title van context		
Relationship	String	Case relatie tot context	Ja	Cluster informatie. Mogelijke determinant van effectiviteit BCO.
Start.Date	Datetime	Eerste dag aanwezig context	Nee	Cluster informatie
End.Date	Datetime	Laatste dag aanwezig context		
Notes	String	Notities over contact met deze context	Nee	Cluster informatie. Mogelijke determinant van effectiviteit BCO.
Details	String	Beschrijving van de context		
Hash_case_identifier	String	Om te linken aan de cases	Ja	

Variabelen uit HPZone – Actions

Variabele	Type	Uitleg	(Bijzonder) persoonsgeven ja/nee	Reden gebruik
Action.Identifier	String	Record identifier	Nee	Cluster informatie
Action.Number	Int			
Status	String	Open/closed	Nee	Indicator doorlooptijd BCO
Progress	String			
Date.created	Datetime	Datum aangemaakt		
Date.opened	Datetime	Datum geopend		
Date.due.for.completion	Datetime	Datum due		
Date.closed	Datetime	Datum gesloten		
Created.by.Identifier	String	Identifier medewerker die action heeft aangemaakt (gehasht)	Ja	Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO
Assigned.Individual.Identifier	String	Identifier medewerker die de actie toegewezen heeft gekregen (gehasht)		
Hash_case_identifier				
Closed.by.Identifier	String	Identifier medewerker die de actie heeft gesloten		
Action	String	Actie title/naam. Actie is bijvoorbeeld 'start BCO', 'bel contact' etc.	Nee	
Days.Due	Int	Aantal dagen totdat de actie voltooid moet zijn		
Item.Type	String	Item type (case etc.)		
Action.for.Identifier	String			

Variabelen uit HPZone – Monitoring calls

Variabele	Type	Uitleg	(Bijzonder) persoonsgeven ja/nee	Reden gebruik
Monitoring Call	String	Titel van monitoring call	Nee	Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO
Monitoring Call_Id	String	Identifier	Nee	Nodig voor behoud data structuur
Call Type	String	Telefoontje gepleegd / telefoontje ontvangen	Nee	Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO
Date and Time	Datetime	Datum monitoring call	Nee	Indicator doorlooptijd BCO
Details	String	Notities monitoring call	Ja	Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO
Temperature	Int	Lichaamstemperatuur	Ja	Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO
Person has symptoms?	String	Heeft cliënt COVID-19 gerelateerde symptomen?		
Date Symptoms Started	Datetime	Wanneer zijn de COVID-19 gerelateerde symptomen begonnen?		
Koorts	Bool (true/false)	Heeft persoon dit symptoom?		
Hoesten	Bool	Heeft persoon dit symptoom?		
Keelpijn	Bool	Heeft persoon dit symptoom?		
Benauwdheid	Bool	Heeft persoon dit symptoom?		
Neusverkoudheid	Bool	Heeft persoon dit symptoom?		
Hash_case_identifier	String	Identifier om case/contact te linken	Ja	Nodig voor behoud data structuur

Variabelen uit HPZone – Investigations

Variabele	Type	Uitleg	(Bijzonder) persoonsgeven ja/nee	Reden gebruik
Specimen Type	String	Keel/neus etc.	Nee	Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO
Test	String	PCR/LAMP etc.		
Laboratory	String	Laboratorium dat de test heeft uitgevoerd		
Source	String	Bron van de case = Coronit. Indien de bron niet CoronIT is dan is het veld leeg		
Date Sent	Datetime		Nee	Indicator doorlooptijd BCO
Time Entered	Datetime			
Notes	String	Notities over test	Nee	Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO
Results	String	Positief/negatief	Ja	Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO
Date of Report	Datetime	Datum	Nee	Indicator doorlooptijd BCO
Client Notified	Bool	Client genotificeerd?	Nee	Indicator doorlooptijd BCO
Date Notified	Datetime	Datum notificatie?	Nee	Indicator doorlooptijd BCO
Notified By_Id	String	Notificatie uitgevoerd door medewerker (gehasht)	Ja	Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO
Type	String	Case/contact	Ja	Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO
Initial Type	String	Case/Contact	Nee	Mogelijke determinant van doorlooptijd corona test/bco keten & effectiviteit BCO
hash_case_identifier	String	Om te linken met case/contact	Ja	Nodig voor behoud data structuur
hash_sample_nr	String	Om te linken met coronit	Ja	Nodig voor koppeling CoronIT/HPZone

Variabelen uit HPZone – Case/situation link table

‘Many-to-many’ linking table om cases aan situations te kunnen linken met behulp van identifiers.

Variabele	Type	Uitleg	(Bijzonder) persoonsgeven ja/nee	Reden gebruik
Case Creation Date	Datetime	Datum aangemaakt	Nee	Nodig voor behoud data structuur
hash_case_identifier	String	Identifier	Ja	
Situation Name	String	Naam situation	Nee	
Situation Number	Int	Situation identifier	Nee	

Variabelen uit HPZone – Case/contact link table

‘Many-to-many’ linking table om cases aan contacten te kunnen linken met behulp van identifiers.

Variabele	Type	Uitleg	(Bijzonder) persoonsgeven ja/nee	Reden gebruik
hash_case_identifier	String	Identifier case	Ja	Nodig voor behoud data structuur
hash_contact_identifier	String	Identifier contact	Ja	
Date Time Entered	Datetime	Wanneer is het contact ingevoerd	Nee	
Positive Case	String	Y/N	Ja	
Contact Category	String	Categorie van contact (1/2/3)	Nee	

Osiris Variabelen

Variable	Type	Uitleg	Persoonsgegevens
STATUS	String		Nee
CREATIEDT	Datetime		Nee
LAATSTEWIJZIGINGDT	Datetime		Nee
VERSIE	Int		Nee
LAATSTEWIJZDOOR	String		Nee
VRAGENLIJSTVERSIE	Int		Nee
MELGGDontvDt	Datetime	Datum ontvangen	Nee
MELGGDEExtern	String		Nee
NCOVberoepAnd	String	Beroep beschrijving	Ja
PATAzc	Int		Ja
NCOVvast1eziektedag	String	Eerste ziektedag bepaling	Ja
ZIE1eZiekteDt	Datetime	Eerste ziektedag	Ja
NCOVdat1ezkhpn	Datetime	Eerste ziekenhuisopname datum	Nee
NCOVgezstatDesc	String	Gezondheidsstatus	Ja
ZIEDtOverlijden	Datetime	Overlijden datum	Nee
NCOVdat1eposncov	Datetime	Eerste positieve test datum	Nee
NCOVpatZhsIndDesc	String	Ziekenhuis opname beschr.	Ja
NCOVberoepDesc	String	Beroeps beschrijving	Ja
NCOVStudentLL	String	Student/scholier	Ja
NCOVNContactCat1	Int	Aantal cat1 contacten	Nee
NCOVNContactCat2	Int	Aantal cat2 contacten	Nee
NCOVNContactCat3	Int	Aantal cat3 contacten	Nee
NCOVpatvacDt	Datetime		Nee
NCOVpatvac1Dt	Datetime	Vaccinatie 1 dt	Nee
NCOVpatvac2Dt	Datetime	Vaccinatie 2 dt	Nee
NCOVpatgebland	String	Geboorteland	Ja
NCOVBtnlndDatTer	Datetime	Datum terug uit buitenland	Nee
NCOVpatvac1Dt_c	Datetime	Datum vaccinatie 1	Nee
NCOVpatvac2Dt_c	Datetime	Datum vaccinatie 2	Nee

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst, Bijlage 5

Herinfectie	String		Ja
Ziekenhuisopname	String		Ja
Ziekenhuisopname_Indicatie	String		Ja
ICU	String		Ja
Overleden	String		Nee
Overleden.Oorzaak	String		Nee
Beroep	String		Ja
Gezondheidsmedewerker	String		Ja
Onderwijsmedewerker	String		Ja
Gezondheidszorg	String		Ja
Onderwijs	String		Ja
Student	String		Ja
Land	String		Ja
Geboorteland	String		Ja
Land_verblijf	String		Ja
Reishistorie	String		Ja
Bron_buiteland	String		Ja
Vaccinatie_uitgenodigd	String		Nee
Gevaccineerd_ja_nee	String		Ja
Vaccinatie_aantal_dosis	Int		Ja
Vaccinatie_doelgroep	String		Ja
Vaccinatie_merk	String		Ja
Vaccinatie_EZD_interval	Int		Nee
Vaccinatie_status_ezd_Desc	String		Ja
Test_zelf_melding	String		Ja
pc4	Int		Ja
Gemeente	String		Nee
GGD	String		Nee
Afspraak_start_datum_CoronIT	Datetime		Nee
Monsternummer (hash)	String		Nee
Instelling	String		Ja
Instelling_type	String		Nee
Bewoner_Verpleeghuis	String		Ja

CONTROL – Gezamenlijke Verwerkersverantwoordelijken Overeenkomst, Bijlage 5

Bewoner_Gehandicaptenzorginstelling	String		Ja
Vaccinatie_doelgroep_c	String		Ja
Vaccinatie_merk_c	String		Ja
BCO	String		Nee
BCO_door_medewerker	String		Nee
BCO_door_index	String		Nee
BCO_CoronaMelder	String		Nee
Gerelateerde_ziektegevallen	String		Nee
Bekende_Bron	String		Nee
ContactInvDt	Datetime		Nee
Tijd_tot_contactinventarisatie	Int		Nee
Contact_inventarisatie_status	String		Nee
Bron_Gerelateerde_geval	String		Ja
Setting (Thuis Werk School Reis Overig Huisarts Ziekenhuis OverigZorg Verpleeghuis Woon_GHZ Woon_Overig Dagopvang Dagopvang_Overig Hospice Kerk Koor Vrijetijd Horeca Bezoek Feest Student Vlucht Uitvaart Onbekend)	Int		Ja
SettingNA	String		Nee
SettingJa_Nee	String		Nee
dagen_tusen_infecties	Int		Nee
herinfectie_bepaling	String		Ja

* Reden van gebruik van de osiris variabelen: het zijn epidemiologisch relevante karakteristieken van personen met een SARS-CoV-2 diagnose. Deze karakteristieken kunnen verklarend zijn voor het risico dat een persoon heeft op het verspreiden van het virus en het effectiviteit van het BCO dat rondom deze persoon wordt uitgevoerd. De variabelen zijn nodig om de kernvragen van het onderzoeksproject CONTROL te beantwoorden.

* In de osiris lijst komen variabelen voor die erg op elkaar lijken. Meestal komt dit doordat er gedurende de looptijd is overgeschakeld van opslag in de ene variabele naar opslag in de andere. Omdat hier mogelijk wat handwerk nodig is voegen we de variabelen in de cloud samen en niet vooraf in een geautomatiseerd script. Ook is er op naam overlap tussen de osiris variabelen en HPZone variabelen waar op eenzelfde manier mee wordt omgegaan.

Bijlage 4. Contactgegevens van Partijen bij Inbreuk in verband met Persoonsgegevens

In het geval van een Inbreuk in verband met Persoonsgegevens wordt dit zo snel mogelijk na constatering kenbaar gemaakt aan de Personen opgenomen in onderstaande lijst:

Partij	Naam	Functie	Email	Telefoon
GGD Amsterdam	5.1.2e	5.1.2e	5.1.2e@ggd.amsterdam.nl	5.1.2e
GGD Amsterdam			5.1.2e@ggd.amsterdam.nl	
GGD Flevoland			5.1.2e@ggdflevoland.nl	
GGD Gelderland Midden			5.1.2e vggm.nl	
GGD Groningen			5.1.2e@ggd.groningen.nl	
GGD Hart voor Brabant			5.1.2e@ggdhvb.nl	
GGD Rotterdam-Rijnmond			5.1.2e@rotterdam.nl	
GGD Regio Utrecht				
GGD Zuid Limburg				

Bijlage 7**AVG compliance assessment anDREa**



GDPR Compliance Assessment

Version:	v0.8
Author	5.1.2e

Table of Contents

1 Introduction	2
2 GDPR Compliance Assessment — General	3
2.1 Lawful basis and transparency	3
2.1.1 What information is processed and who has access to it	3
2.1.2 Legal justification for data processing activities	4
2.1.3 Clear information about data processing and legal justification in privacy policy	4
1.2 Data security	5
1.2.1 Data protection from developing to processing	5
3. GDPR Compliance Assessment — Detailed	6
3.1 Governance	6
3.2 Privacy Notices	7
3.3 Fair Processing	8
3.4 Data Subject Rights	9
3.5 Privacy by Design and Default	10
3.6 International Data Export	11
3.7 Security	12
3.8 Data Breach Procedures	13



1 Introduction

The purpose of this document is to describe anDREa's compliance with the GDPR. This document also describes in what way anDREa unburnes de Azure DRE Tenants and the Accountables of Workspaces in being demonstrably compliant with the GDPR.

The statement of GDPR Compliance Assessment is based on the [GDPR Compliance Checklist of appknox](#).

This document will be updated at least annually and when significant change happens to the relevant areas covered.

2 GDPR Compliance Assessment — General

2.1 Lawful basis and transparency

2.1.1 What information is processed and who has access to it

Organizations that have at least 250 employees or conduct higher-risk data processing are required to keep an up-to-date and detailed list of their processing activities and be prepared to show that list to regulators upon request.

The list should include: the purposes of the processing, what kind of data is processed, who has access to it in your organization, any third parties (and where they are located) that have access, what you're doing to protect the data (e.g. encryption), and when you plan to erase it (if possible).

Azure DRE does not provide evidence of:

Azure DRE does not provide evidence of	However, this can be found in
Full list of studies	Study Registry
The purpose of the processing	Ethical Commission approval, Data Management Plan, Study Registry
What kind of data is processed	Data Management Plan
Location of the third parties	Processing agreement
When you plan to erase the data	Data Management Plan

Azure DRE does provide evidence of

Azure DRE does provide evidence of	This can be found in
Who has access (incl. third parties)	Access to a Workspace is restricted to members, logging of the history is available
What is done to protect the data	- Only authorized users/processes have access to a Workspace - Users are required username, password and 2FA - Data is encrypted in-transit - Data is encrypted at-rest - Data resides in Microsoft Azure Data Centers in the EUR
Erasing data	When a Workspace is deleted, all the data is deleted. Erasure of data on the Data Share comes really in effect when the 30-day rolling snapshot passes after deletion, and any backups prior to the erasure of data are deleted.

2.1.2 Legal justification for data processing activities

Processing of data is illegal under the GDPR unless you can justify it according to one of six conditions listed in [Article 6](#). There are other provisions related to children and special categories of personal data in [Articles 7-11](#). Review these provisions, choose a lawful basis for processing, and document your rationale. Note that if you choose "consent" as your lawful basis, there are [extra obligations](#), including giving data subjects the ongoing opportunity to revoke consent. If "legitimate interests" is your lawful basis, you must be able to demonstrate you have conducted a privacy impact assessment.

Azure DRE does not provide evidence of:

Azure DRE does not provide evidence of	However, this can be found in
Any legal justification, nor the lawfulness for processing of data in a Workspace	Ethical Commission Approval, Informed Consent of participants

Azure DRE does provide evidence of:

Azure DRE does provide evidence of	This can be found in
Legal justification and the lawfulness for processing Azure DRE user information	The logging of the consent people give before their account has been created.

2.1.3 Clear information about data processing and legal justification in privacy policy

You need to tell people that you're collecting their data and why ([Article 12](#)). You should explain how the data is processed, who has access to it, and how you're keeping it safe. This information should be included in your [privacy policy](#) and provided to data subjects at the time you collect their data. It must be presented "in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child."

Azure DRE does not provide evidence of:

Azure DRE does not provide evidence of	However, this can be found in
Clear information about data processing in a Workspace	Data Management Plan, Informed Consent
Legal justification in privacy policy that applies to a the data in a Workspace	Informed Consent
Clear information about data processing of subject data in a Workspace	Data Management Plan, Informed Consent, Study Proposal, Study Management System

Azure DRE does provide evidence of:

Azure DRE does provide evidence of	This can be found in
Clear information about data processing of User Account data	Cookie Policies
Legal justification in privacy policy for User Account data	Privacy Policy

1.2 Data security

1.2.1 Data protection from developing to processing

You must follow the principles of "[data protection by design and by default](#)," including implementing "appropriate technical and organizational measures" to protect data. In other words, data protection is something you now have to consider whenever you do anything with other people's personal data. You also need to make sure any processing of personal data adheres to the data protection principles outlined in [Article 5](#). Technical measures include encryption, and organizational measures are things like limiting the amount of personal data you collect or deleting data you no longer need. The point is that it needs to be something you and your employees are always aware of.

Azure DRE does not provide evidence of:

Azure DRE does not provide evidence of	However, this can be found in
Implemented appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects	Data Management Plan, Study Management System

Azure DRE provides evidence of:

Azure DRE does provide evidence of	This can be found in
Who was allowed to access the data in what role, who accessed the Workspace, who requested egress, who approved egress, who egressed when what, who approved opening specific outbound ip-address access.	Azure DRE Logging

3. GDPR Compliance Assessment — Detailed

3.1 Governance

Actions	Description	GDPR Article(s)	Implementation in Azure DRE	Not anDREa responsibility
Record keeping	Maintain records of the controller and Data Protection Officer (if applicable). Maintain categories of data, logs of transfers. Wherever possible add descriptions of possible measures taken to ensure security.	Article 30	Azure DRE maintains records of: • Workspace membership • Data transfer using Portal	• Maintaining records of the controller and Data Protection Officer is the responsibility of the Tenant • Maintaining categories of data (e.g. in Data Management Plan, research management tool) is the responsibility of the PI
Data Protection Officer (DPO)	Establish whether the company is required to have a DPO. If the company is not required to have a DPO, you may appoint a voluntary DPO. DPO contact details must be notified to the regulatory authority and published to the public.	Article 37	N/a. AnDREa is not required to have a DPO. The role CTO takes care of the responsibilities of the DPO	• A DPO (FG, Functionaris Gegevensbescherming) is the responsibility of the Tenant
Employee Training	Employees who handle personal data of either customers or other employees must be trained to handle it according to GDPR principles.	Article 5	Data Handling Policies	• The role Accountable in a Workspace is responsible to ensure that all the members are trained in GDPR principles
Policies and Procedures	There is a list that covers different policies and procedures. There is no fixed way to handle this but it should be done according to what is applicable for your business. Some of the items on the list are: • General Data Protection Policy • Data Subject Access Rights Procedure • Data Retention Policy • Data Breach Escalation and Checklist • Employee Privacy Policy and Notice • Processing customer data policy • Guidance on privacy notices	Article 5	• General Data Protection Policy • Data Subject Access Rights Procedure • Data Retention Policy • Data Breach Escalation and Checklist • Employee Privacy Policy and Notice • Processing customer data policy • Guidance on privacy notices	Tenant/Accountable is responsible for data subjects in a Workspace.

3.2 Privacy Notices

Privacy notices basically put emphasis on the transparency requirement of GDPR. All notices issued must be information, concise and clear. Employees and customers need to be adequately informed of all data processing activities and information set out in Articles 14 and 14 must be provided.

Actions	Description	GDPR Article(s)	Implementation in Azure DRE	Tenant responsibility
Issue notices at the right time	Notices must be given at the time that the data is obtained from the data subject, or if the data was received from a third party, within a reasonable period after obtaining the data but at the latest within one-month	Articles 12-14	anDREa does not receive user data from third parties. People will only be onboarded as users if they explicitly agree.	Tenant/Accountable is responsible to give notice to data subjects whose data is being processed in a Workspace.
Be complete and concise	Notices must be complete and provide all the required information, like the identity of the controller, purpose of processing, duration, consent, right to withdraw consent, etc.	Articles 12-14	The information for potential users of the Azure DRE is complete and concise.	Tenant/Accountable is responsible for data subjects in a Workspace.
Easy to understand and comprehend	The format of the notice should be easy to read, handle and understand	Articles 12-14	The information for potential users of the Azure DRE is easy to understand and comprehend.	Tenant/Accountable is responsible for data subjects in a Workspace.

3.3 Fair Processing

The Fair Processing category means that in order to lawfully process personal data, the conditions of processing must be met. This category is pretty much similar to what the processing rules were in the current Data Privacy Directive except for a few new requirements.

Actions	Description	GDPR	Implementation in Azure DRE	Tenant responsibility
Establish a legal basis for processing all the personal data that you hold	As a business, you need to be able to provide evidence that you have a legal basis to own and process personal data that you hold. Consent from the data subject, the legal obligation of the controller, and special care where data is that of a child is necessary.	Articles 5, 6, 7, 9, 10, 85 to 91	For Azure DRE users this is part of the onboarding procedure.	Ensure informed consent of each participant, or have an approval to work without informed consent
Profiling	A few questions to answer here: • Does your company carry out profiling on employees or customers? • If so, does this profiling result in making a decision about the individual which would have a significant legal effect or similar on that individual e.g. refusal of credit or refused for an interview? • If the answer to (b) is yes, does your Company have the consent of the individuals to this profiling?	Articles 5, 6, 7, 9, 10, 85 to 91	anDREa does not profile employees or users.	Conduct a DPIA per Study
Children	If your business processes personal data of children, then consider the language used for privacy notices and plan out how to obtain valid consent from parents/guardians.	Articles 5, 6, 7, 9, 10, 85 to 91	anDREa users are 16+	Ensure compliance with these articles

3.4 Data Subject Rights

Current data subject rights require you to request access to data when you need it, rectify it or delete it. Under GDPR, it's not just the right to access data but also provide it in a machine-readable format, also called data portability.

Actions	Description	GDPR Article(s)	Implementation in Azure DRE	Tenant responsibility
Data subject access right	As a company, are your employees or customers allowed to get access to their personal data processed by your company? Do you have employees that have been trained to respond to such requests within the stimulated timeframe of 1 month?	Article 15	When requested, andREa can and will provide access to their personal data processed by andREa and as a general rule of thumb this will be done within 1 month after a written request.	Tenant/Accountable is responsible for any requests regarding subjects whose data resides in a Workspace.
Processed to allow subjects to exercise their rights	This basically understands if as a company you have the technology and processes in place to allow data subjects to exercise their rights like the right to erasure, data portability, restriction of processing, and right to object.	Article 16-21	When requested andREa can and will remove user account information. User interaction in logging will be retained for compliance requirements.	Tenant/Accountable is responsible for any requests regarding subjects whose data resides in a Workspace.

3.5 Privacy by Design and Default

One of the major objectives of GDPR is to bring privacy consideration to the forefront of every organization. The GDPR requires data protection requirements to be considered when [new technologies](#) are designed or on-boarded or new projects using data are being considered. You should ensure that you perform an assessment to understand the impact to privacy as you onboard new projects.

Actions	Description	GDPR Article(s)	Implementation in Azure DRE	Tenant responsibility
Privacy by design	The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures in an effective manner. The controller is responsible to integrate the necessary safeguards into the processing in order to meet the requirements of this regulation and protect the rights of data subjects	Article 25	All data is and only is roll based accessed and requires username, password and 2FA.	All data is and only is roll based accessed and requires username, password and 2FA. For all data in a Workspace the Tenant or Accountable is the controller.
Privacy by default	The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.	Article 25	The minimum amount of Azure DRE user data is processed: name, email, phone number, membership of what Workspaces in what role, activities such as but not limited to: ingress, access, egress, add/remove members, add/remove resources, start/stop resources. Data Handling Policy	For all data in a Workspace the Tenant or Accountable is the controller.

3.6 International Data Export

Under the International Data Export rule of the GDPR, companies are permitted to export data within its group and third-party vendors outside the European Economic Area (EEA) if the country in which the recipient of such data is established offers an adequate level of protection.

Actions	Description	GDPR Article(s)	Implementation in Azure DRE	Tenant responsibility
Group companies or third-party vendors	If you use group companies or third-party vendors to process data, there must be a written contract with each one of them validating that they meet the expectations set out in Article 28.	Article 28	anDREA does not use group companies or third-party vendors to process user data.	If a Workspace uses resources outside the EEA (by default it is within EEA), the necessary written contracts have to be in place.
Transferring data out of EEA	If you are exporting data outside of EEA, you need to follow an approved transfer mechanism, which includes one of the following: A. a country which has a finding of adequacy from the European Commission B. If it is within The Company group, are binding corporate rules in place? C. Standard contractual clauses as approved by the European Commission D. If the transfer is to the US, on the basis of the Privacy Shield. E. With the consent of the data subject. F. The transfer is necessary to carry out a contract with the data subject G. The transfer is in the public interest H. The transfer is necessary to establish, exercise or defend legal rights I. The transfer is necessary to protect the vital interests of a person where the data subject is physically or legally incapable of giving consent.	Articles 44-49	anDREA, if at all, will only transfer data to another site on explicit instruction of a Tenant or Accountable person.	• Tenant or Accountable is responsible for complying to Articles 44-49 if applicable. • Usually this is part of Data Transfer Agreements made with receiving parties

3.7 Security

Actions	Description	GDPR Article(s)	Implementation in Azure DRE	Tenant responsibility
Appropriate security measures for personal data	<u>Security</u> has to be appropriate to the likely risks to individuals if data was lost, stolen or disclosed to unauthorized people. It is important to note here that the security covers both organizational as well as technical measures. Some factors to consider are: • Pseudonymisation • Encryption • Ensuring ongoing integrity, confidentiality, availability and resiliency • The ability to restore in a timely manner • Processes for testing security	Article 32	• Data is encrypted at rest • Data is encrypted in transit • 30-day rolling snapshots are made of the data that can be self-serviced restored • Azure DRE / Shared Tenant code lifecycle follow a strict procedure • Azure DRE is classified for Integrity (of data) as MEDIUM, found suitable for most studies • Azure DRE is classified for Availability MEDIUM, found suitable for most studies	• Pseudonymisation, encryption is the responsibility of the PI/Tenant • Workspace members are responsible for checking the data ingress, processing, and egress fitting the classification for Integrity (of data) as MEDIUM, found suitable for most studies • Workspace

3.8 Data Breach Procedures

As part of the new GDPR compliance checklist is a data breach notification rule. The process requires organizations to act quickly, mitigate losses and, where mandatory notification thresholds are met, notify regulators and affected data subjects.

Actions	Description	GDPR Article(s)	Implementation in Azure DRE	Tenant responsibility
Mandatory notification	Do you have the necessary procedures in place to report a breach within 72 hours of becoming aware of it? The breach has to be investigated and details provided to the regulator and mitigations have to be taken to address it.	Article 33	Data Breach Procedure This expanded with notification to Azure DRE Tenant(s) in case anDREa is aware of a (potential) data breach of one or more of their Workspaces	• Tenant remains Controller of data residing in Workspaces • Data Breaches affecting the Tenant will be notified to the Tenant appointed person(s)
Notification to affected individuals	If the breach is likely to result in a high risk to the rights and freedoms of individuals, the company will need to notify the individuals affected. Only if the data is encrypted or otherwise unintelligible, then individuals will not need to be notified.	Article 34	Part of the Data Breach Procedure This expanded with notification to Azure DRE Tenant(s) in case anDREa is aware of a (potential) data breach of one or more of their Workspaces	• Tenant remains Controller of data residing in Workspaces • Data Breaches affecting the Tenant will be notified to the Tenant appointed person(s)

Bijlage 8

DPIA anDREa



Data Protection Impact Assessment

Version:	v1.0
Author	5.1.2e

Table of Contents

1 Introduction	2
2 Data Protection Impact Assessment	3
2.1 Identify the need for a DPIA	3
2.2 Describe the process	3
2.3 Consultation process	6
2.4 Assess necessity and proportionality	7
2.5 Identify and assess risks	8
2.6 Identify measures to reduce risk	9
2.7 Sign off and record outcomes	10



1 Introduction

anDREa is committed to the GDPR.

The purpose of this document is to describe anDREa's Data Protection Impact Assessment (DPIA).

The template used for the DPIA: [Sample DPIA template](#) from [ico](#)

This document will be updated at least annually and when significant change happens to the relevant areas covered.

2 Data Protection Impact Assessment

2.1 Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

The Azure DRE Shared Tenant provides organizations, after entering an agreement with anDREa these organizations are called Tenant, the opportunity to associate one or more of their Microsoft Azure Subscriptions with the AAD of anDREa.

This makes it possible to deploy Workspaces on instructions of the Tenant with minimally one person mandated by the Tenant and having an account of the Tenant in the role of Accountable.

A Workspace allows to ingress, process, analyse, and egress data in a safe way with one or more people, not necessarily having an account of that Tenant.

2.2 Describe the process

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?

When a person is invited to become a new user to Azure DRE, that user has to agree with [Terms of Service](#) and [Privacy Policy](#) before an account is created for that user.

User data will be stored in the AAD of anDREa (name, email, phone number), this information is provided by other users or the Tenant.

anDREa will not share user data with third parties. See [Data Handling Policy](#)

All data, be it of the Shared Tenant or in the Workspaces, is encrypted at-rest and in-transit and is only role-based accessible; user data and data in Workspaces.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Data processed by anDREa:

- As part of the proposition of anDREa it is important that all relevant user activities are logged. anDREa uses [Assessment Framework for Services](#) as to what data must be logged.
- Data processed is:
 - name, email and phone number
 - No special category or criminal offence data is processed
- anDREa does not collect more data than it needs or is mandated to
- The number of users enrolled on Azure DRE is how many individuals are affected
- Azure DRE users can reside in any part of the world

Data processed by Accountable of a Workspace:

anDREa's proposition is to provide users the ability to ingress, process, analyse, and egress privacy sensitive data in a Workspace. anDREa does not know what kind of data is residing in Workspaces and therefore it is assumed that one or more Workspaces will contain highly privacy sensitive information at any given time. **As such Accountables are responsible for conducting the DPIA for their Workspaces and involve the necessary parties including but not limited to DPO of their Tenant.**

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Data processed by anDREa:

- Is that of users of Azure DRE
 - All users are 16+ and are considered not vulnerable
- The rights of users are stipulated in the [Data Protection Policy](#)
- anDREa works in accordance of:
 - ISO 27001
 - GDPR
- anDREa intends to get certified
- anDREa is in the process of expanding to work in accordance of:
 - ISO 9001
 - NEN 7510

Data processed by Accountable on Azure DRE:

- anDREa ensures that the default Workspace is secure and no data can be ingressed in or egressed out of the Workspace without explicit membership of that Workspace. Egress requires approval of at least the role Privileged Member; who is allowed to have the role Privileged Member is determined by the Accountable. Any requested or self service functionality that will make the Workspace workable for the specific situation but might decrement the auditability and security requires explicit opt-in from at least the role Privileged Member.
- As such, **Accountables are responsible for conducting the DPIA for their Workspaces and involve the necessary parties including but not limited to DPO of their Tenant.**

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you, and more broadly?

Azure DRE user data is processed for:

- Azure DRE usage
- Demonstrable compliant for anDREa
- Demonstrable compliant & risk assessments for Tenants
- Demonstrable compliant for Accountable

Accountables and the members in their Workspace process data for:

- The purpose as is approved in the organization of the Accountable
- The benefits are that of the Accountable and Tenant, anDREa has no benefit of the processed data

2.3 Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

The consultation process involves:

- CISO's of Tenants
- Community representatives
- Core Support Team - employees of Tenants
- Direct interaction with people having the role of Accountable and Privileged Member
- anDREa developers

2.4 Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Data processed by anDREa:

For a correct functioning of the Azure DRE and providing the demonstrable evidence of compliance it is necessary that user interactions with the Azure DRE are being logged. Name, email and phone number are necessary for safe and demonstrable evidence of compliance.

Function creep is assured that storing data costs money and requires maintenance. Cost reduction of operations is a key metric for anDREa.

Data processed by Accountable on Azure DRE:

The organization of the Accountable is responsible to safeguard the lawful basis for processing of the Accountable and what follows. This includes but is not limited to ensure Data Transfer Agreements are in place when data is given to others including international transfers.

2.5 Identify and assess risks

ID	Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
For anDREa				
1	People no longer involved with anDREa can still access anDREa code, Sharepoint, email, Teams of anDREa.	L/M	H	H
2	Unauthorized access to compute, storage or other resources	M	H	H
3	Unauthorized physical access to data carriers	L	H	H
4	Using 'skeleton' keys on Azure	L	H	H
5	Denial of Service attacks	M	H	H
For Accountable				
6	People no longer involved with the Workspace have still access	M	H	H
7	RDP brute force attacks on VMs used	M	H	H
8	Uploading compromised software	M	H	H
9	Attacks via open ports	L	H	H
10	Unintentional egress of data from Workspace	M	H	H

2.6 Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk ID	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
For anDREa				
1	anDREa has an active policy to revoke access based on least-privilege. Access of people no longer involved in anDREA will be revoked within 5 working days.	H	L	Yes
2	• Active monitoring on deviations • Username, password, 2FA • Access-on-demand for critical resources	H	L	Yes
3	• Data in workspace is encrypted at-rest • Microsoft Azure Policies	H	L	Yes
4	Always 2FA (except for non-used break-the-glass account), ADDS	H	L	Yes
5	24/7/365 active monitoring	H	L	Yes
For Accountable				
6	Accountable / Privileged Members revoke self-service access of members no longer involved in the work	H	L	Yes
7	• VM access requires IP-address whitelisting; on-prem this is the default, off-prem this can only be done after using 2FA • 24/7/365 monitoring • Default a VM is deallocated around 19:00 CET, upon restart a new public IP is given	H	L	Yes
8	Windows defender is standard up-to-date in the VMs 30 day rolling 24h snapshot	H	L	Yes
9	• Outbound only • Easy to turn on/off rule • Clear warning before the rule can be turned on	L	L	Yes
10	• Default workspace is through an authorization Workflow • Alternatives (e.g. via outbound open port) are accompanied with clear formulation of risks and have to be accepted before they become active	M/H	L	Yes

2.7 Sign off and record outcomes

Item	Name	Date
Measures approved by:	5.1.2e andREa	17-8-2020
Residual risks approved by:	5.1.2e andREa	17-8-2020
DPO* advice provided:	5.1.2e andREa * anDREa is not required to have a DPO	17-8-2020
Summary of DPO* advice: User account data is well protected from a privacy point of view as intended by the GDPR. As for Azure DRE users: • As long as the users are keeping to the Terms of Service • Does the Azure DRE Shared Tenant Workspaces provide an equal and usually the best alternative • To ingress, process, analyse, and egress data that are privacy sensitive in nature • With tooling of the user choosing • In collaboration with externals if required • With relevant logging as demonstrable evidence for compliance		

Bijlage 9

Toetredingsformulier GGD Gelderland Midden

159 - 159

Dubbel