Gegevensbeschermings-effectbeoordeling

(Privacy Impact Assessment)

VWS, RIVM, I&V, EPI, RES/MOD

PIA t.b.v. Infectieradar

Bilthoven, 11-11-2022

Vaststelling verwerkingsverantwoordelijke
Naam: 5.1.2e

Datum: 12-12-2022

Advies 5.1.2e 5.1.2e
Naam: 5.1.2e

Datum:

Contact:

Ministerie van Volksgezondheid, Welzijn en Sport,

Parnassusplein 5
2511 VX Den Haag

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

5.1.2e RIVM/CIb/EPI/RES

5.1.2e @rivm.nl

Inhoudsopgave

A. Beschrijving kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

Onder A wordt de eerste stap beschreven van de DPIA: een overzicht van alle relevante feiten van de voorgenomen gegevensverwerkingen. Essentieel is dat de feiten helder en volledig zijn, want het resterende deel van de DPIA is gebaseerd op wat in dit onderdeel is beschreven.

1. Voorstel

Beschrijf het voorstel waar de DPIA op toeziet op hoofdlijnen en benoem hoe het voorstel tot stand is gekomen en wat de beweegredenen zijn achter de totstandkoming van het voorstel.

Deze Gegevensbeschermingseffectbeoordeling (hierna: PIA) is bedoeld voor het wetenschappelijk onderzoek op het gebied van de verspreiding van infectieziekten en de huidige Corona uitbraak in het bijzonder. Deze studie wordt uitgevoerd door het Epidemiologie Centrum en Surveillance (EPI) van het RIVM.

Het doel van dit onderzoek is het bestuderen van gezondheidsklachten die kunnen wijzen op infectieziekten. Dit onderzoek is van cruciaal belang om vrijwel real-time te monitoren of het aantal mensen met klachten door een infectieziekte, zoals COVID-19, toeneemt of afneemt, en dat te relateren aan het al dan niet versoepelen van maatregelen tegen verspreiding.

De gegevens voor dit onderzoek worden verzameld via RIVM Infectieradar. Het onderzoek is al eerder gestart in maart 2020, gebruikmakend van de naam Infectieradar maar met andere software en verwerkingen, welke zijn beschreven in afzonderlijke PIAs (van 13 maart 2020 en 13 mei 2020). De onderstaande PIA ziet toe op de nieuwe software en verwerking die worden gebruikt bij de huidige versie van Infectieradar. Deze nieuwe versie heeft de naam RIVM Infectieradar. Het reeds gestarte onderzoek onder de oude versie van Infectieradar veranderd niet met de overgang naar deze nieuwe software en de doelstelling van het onderzoek blijft hetzelfde. Daarom worden de persoonsgegevens die via de eerdere versie(s) van Infectieradar zijn verzameld, ook voor dit onderzoek gebruikt. Een relevant verschil tussen RIVM Infectieradar en haar voorgangers is dat er voor hosting geen gebruik wordt gemaakt van externe partijen, er een hogere mate van beveiliging en databeveiliging is en er een betere workflow is wat betreft het versturen van vragenlijsten en het beheer van de database. Dit betekent dat er nu een front-end aanwezig is waarop deelnemers kunnen inloggen, en hun data kunnen beheren en vernieuwen.

RIVM Infectieradar gebruikt software ontwikkeld door Coneno, een softwarebedrijf gelinkt aan het academische instituut DFKI in Duitsland. Deze software is ontwikkeld in opdracht van het ISI-foundation in Italië ten behoeve van het samenwerkingsproject Influenzanet en wordt bekostigd uit fondsen van de Europese Commissie (Project "EpiPose"). De software is in beheer van het RIVM, geïnstalleerd op het OpenShift-platform, en is volledig onafhankelijk.

RIVM Infectieradar maakt voor de beveiliging gebruik van Google reCaptcha. Google verwerkt hiervoor als zelfstandig verwerkingsverantwoordelijke een aantal gegevens die gebruikt worden voor het goed functioneren van de dienst (herkennen menselijke gebruikers) en ter verbetering van deze dienst. Gebruik van Google reCaptcha valt echter buiter de scope van de PIA, omdat dit een (generieke) beveiligingsmaatregel is en daarmee losstaat van deze studie naar infectieziekten. Hiervoor is ook een risicoacceptie gevolgd.

Onderdeel van deze PIA zijn diverse bijlagen en proccedures. Waar relevant wordt in de tekst naar een bijlage of procedure verwezen voor nadere of verdiepende informatie. Op pagina 27 is een overzicht van alle bronbestanden opgenomen.

2. Persoonsgegevens

Beschrijf alle persoonsgegevens op die worden verwerkt. Classificeer deze persoonsgegevens naar: gewoon, gevoelig, bijzonder, strafrechtelijk en wettelijk identificatienummer. Geef per categorie betrokkenen aan welke (categorieën) persoonsgegevens worden verzameld.

De deelnemers hebben de mogelijkheid om vragen die onder andere over gezondheidsgegevens te beantwoorden "Dit wil ik niet aangeven". Zie **Bijlage 3a** en **Bijlage 3b** voor een meer precieze indicatie van de opgevraagde gegevens.

De onderzoeksgegevens worden gepseudonimiseerd verwerkt (**zie Bijlage 1**).

Aard rechthebbende

De betrokkenen op wie de gegevens betrekking hebben zijn deelnemende burgers van 16 jaar of ouder. Deelnemers hebben de mogelijkheid om als wettelijk vertegenwoordiger ook gegevens van gezinsleden jonger dan 16 jaar te registreren

Categorie betrokkenen	Categorie persoonsgegevens	Persoonsgegevens	Type persoonsgegeven	Bron/toelichting
Betrokkene*	Inloggegevens	• E-mailadres • Wachtwoord • UserID	Algemeen	- Noodzakelijk voor het aanmelden als unieke gebruiker: - Noodzakelijk voor het toesturen van de wekelijkse reminder voor het invullen van de wekelijkse vragenlijst.
	Demografische gegevens	• PC4 (algemeen) • Jaar en maand van geboorte (algemeen) • Opleidingsniveau (algemeen) • Werk (algemeen) • Gezinssamenstelling (algemeen)	Algemeen	**Vier cijfers postcode:** De 4 cijfers van de postcode zijn noodzakelijk voor wetenschappelijk onderzoek en het monitoren en in kaart brengen van de geografische verspreiding van infectieziekten, zodat bijvoorbeeld regionale verschillen meegenomen kunnen worden en de uitbraak geografisch inzichtelijk kan worden gemaakt voor de verschillende organisatorische niveaus binnen de overheid (gemeente, GGD-regio, veiligheidsregio, provincie etc.). Op basis van die informatie kunnen gerichte maatregelen getroffen worden.

				Maand en jaar van geboorte: - Noodzakelijk voor wetenschappelijk onderzoek en om onder andere inzicht te krijgen in verschillen in verspreiding van het virus binnen de leeftijdscategorie, de symptomen per leeftijd, en de zorgvraag en reporting delay per leeftijd - Noodzakelijk om inzicht te verkrijgen hoe de bevolkingssamenstelling in het panel overeenkomt met de Nederlandse bevolking. **Opleiding, werk en gezinssamenstelling:** - Noodzakelijk om inzicht te verkrijgen hoe de bevolkingssamenstelling in het onderzoek overeenkomt met de Nederlandse bevolking. - Noodzakelijk om inzicht te verkrijgen in de demografische verspreiding van het virus
	Gezondheidsgegevens	• Medische risicogroep (bijzonder) • Test uitslagen Infectieziekten (bijzonder) • Symptomen (bijzonder) • Zwangerschap (bijzonder) • Klinische risicogroep voor vaccinatie (bijzonder) • Vaccinatie (bijzonder)	Bijzonder	**Medische risicogroep en testuitslag infectieziekte:** - Noodzakelijk voor monitoren ziekte beeld om na te gaan of er sprake is van mogelijke verspreiding infectie. - Noodzakelijk voor vaststelling risicogroepen onder andere voor focusbepaling beheers strategie. **Symptomen, zwangerschap en klinische risicogroep voor vaccinatie:** Noodzakelijk voor bepaling impact symptomen en onderliggende oorzaak op het leven van de patiënt. iv.om inzicht te verkrijgen in de zorgvraag door de patiënt en de bepaling van het tijdsbestek voordat een patiënt daadwerkelijk

				zorg vraagt na het begin van de eerste symptomen.
	Loggegevens	• UserID en/of e-mailadres (wat relevant is voor de log)	Algemeen	

3. Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer en geef aan welke persoonsgegevens worden verwerkt per voorgenomen gegevensverwerking. Desgewenst kan een stroomschema van de gegevensverwerkingen worden toegevoegd.

De dataflows staan beschreven in "Infectieradar-flows beschrijving" en zijn visueel weergegeven in "Infectieradar-flows" *(zie Bijlage 2b en Bijlage 2a)*. Ter aanvulling is er ook de systeemdecompositie v6 en de PSA RIVM Infectieradar *(zie Bijlage 1 en Bijlage 2)*, en alle procedure documenten *(zie Procedure 0) toegevoegd*.

4. Verwerkingsdoeleinden

Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

Het doel van de studie en de daaruit voortvloeiende verwerkingen is het bestuderen van gezondheidsklachten die kunnen wijzen op infectieziekten, in het kader van onderzoek zoals bepaald in artikel 3 Wet op het RIVM. Dit gebeurt op basis van het verzamelen van persoonsgegevens die deelnemers vrijwillig via RIVM Infectieradar kunnen registreren.

De onderzoeksresultaten van dit onderzoek helpt bij het monitoren van infectieziekten onder de Nederlandse bevolking, het nemen van passende volksgezondheidsmaatregelen via het landelijke preventie- en mitigatiebeleid en het geven van informatie en advies over de ontwikkeling van infectieziekten aan belanghebbenden, waaronder de Minister van Volksgezondheid, Welzijn en Sport.

De doeleinden voor de verzamelde gegevens is ook verder uitgewerkt in de tabel in H2.

---

5. Betrokken partijen

Benoem alle organisaties die betrokken zijn per voorgenomen gegevensverwerking. Deel deze organisaties in onder de rollen: verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke, verwerker, sub-verwerker, verstrekker, ontvanger en derde. Benoem ook welke functies/afdelingen binnen deze organisaties toegang krijgen tot persoonsgegevens. Voeg aanvullende informatie toe in het tekstveld.

VERWERKINGSVERANTWOORDELIJKE

RIVM

De verantwoordelijke voor de verwerkingen is de Minister van Volksgezondheid, Welzijn en Sport. De gedelegeerd verantwoordelijke is de Directeur-Generaal van het RIVM. RIVM heeft RIVM Infectieradar in eigen beheer en is verantwoordelijk voor de verwerkingen zoals beschreven in deze PIA.

De onderzoekers van het RIVM coördineren de studie, bundelen de gegevens, en voeren de analyses uit. Onderzoekers hebben alleen toegang tot gepseudomiseerde onderzoeksgegevens van deelnemers.

Uitsluitend zes systeembeheerders van het RIVM, die direct betrokken zijn bij RIVM Infectieradar, hebben via de back-end toegang tot de door de deelnemers verstrekte persoonsgegevens. Gepaste procedures zijn opgesteld voor deze systeembeheerders.

PIENTER

RIVM Infectieradar heeft een samenwerking met het PIENTER onderzoek wat ook wordt uitgevoerd door het RIVM. Deelnemers aan PIENTER worden ook uitgenodigd om deel te nemen aan Infectieradar. Deze deelnemers worden op dezelfde manier uitgenodigd als de huidige gebruikers van Infectieradar. Het PIENTER team levert hiervoor een e-mail/ID lijst aan bij de applicatiebeheerder van Infectieradar, die deze gegevens toegevoegd aan het mailingprotocol van Infectieradar. Aansluitend ontvangen deze personen een uitnodiging tot deelname aan Infectieradar. Ten behoeve van het PIENTER onderzoek kunnen onderzoeksgegevens van Infectieradar op verzoek van het PIENTER onderzoek verstrekt worden, maar slechts van deelnemers die aan het PIENTER onderzoek deelnemen. Het PIENTER team ontvangt en verwerkt deze gepseudonimiseerde onderzoeksgegevens als zelfstandig verwerkingsverantwoordelijke.

Europees onderzoek: Influenzanet

De gepseudonimiseerde onderzoekgegevens worden in de toekomst gedeeld binnen een Europese database ten behoeve van het Europese onderzoek van Influenzanet. De data die worden gedeeld zijn bewerkt om indirecte herleidbaarheid verder uit te sluiten. De postcode 4 informatie zal in dit geval worden vervangen door regio (NUTS3 of lager) en de leeftijd wordt vervangen door een leeftijdscategorie. Hierdoor wordt beoogd (in)directe herleidbaarheid van de gegevens te voorkomen. Influenzanet verwerkt de verder gepseudonimiseerde onderzoeksgegevens als zelfstandig verwerkingsverantwoordelijke.

Vanwege de aard van de te verstrekken gegevens is er een data sharing agreement met alle partijen binnen Influenzanet die voorziet in waarborgen voor toepassing en naleving van de GDPR -richtlijnen en specificeert wat de deelnemende partijen wel en niet mogen doen met de data, en hoe besloten wordt welke analyse kan worden uitgevoerd op deze Europese dataset. Door middel van deze overeenkomst wordt dus verder verankerd dat op delen van deze onderzoekgegevens altijd de GDPR -richtlijnen van toepassing zijn.

VERWERKER

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

Coneno

Dit is een Duitse organisatie die op Europees initiatief de software voor infectieradar heeft ontwikkeld (zie Bijlage 7: Referentie onderzoek Coneno). Zij doen nu de doorontwikkeling speciaal voor het RIVM in het kader van RIVM Infectieradar. Coneno is verantwoordelijk voor de technische ontwikkeling van d software, en heeft in die hoedanigheid geen toegang tot verzamelde persoonsgegevens. De software is inmiddels in beheer van het SSC-campus.

Google reCaptcha

6. Belangen bij de gegevensverwerking

Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenomen gegevensverwerkingen. Voeg aanvullende informatie toe in het tekstveld.

Betrokken Partij	Belangen
Algemeen belang	Het algemene belang van dit onderzoek is meer inzichten krijgen in de ontwikkeling van infectieziekten, en om volksgezondheidsmaatregelen te nemen ter bescherming tegen infectieziekten door meer kennis en inzicht uit het onderzoek op basis van verstrekte gegevens. Bij grootschalige uitbraken van infectieziekten is verlichting door ziektemonitoring van de belasting van de zorginfrastructuur een belang. Dit is zowel op nationaal niveau, als ook op internationaal niveau.
RIVM	Het RIVM heeft als belang het uitvoeren van wetenschappelijk onderzoek met als doel het bewaken en bevorderen van de volksgezondheid op het gebied van infectieziekten. Onderdeel hiervan vormt het monitoren van infectieziekten binnen de Nederlandse samenleving. Deze belangen zijn onlosmakelijk verbonden met het doel en de kerntaken van het RIVM.
Betrokkenen	Het belang van de betrokkene is om meer inzicht te krijgen in het verloop van C-19.
ECDC/WHO	Om bij te dragen aan kennis op Europees niveau werken we samen binnen het Influenzanet samenwerkingsverband. Influenzanet rapporteert internationaal vergelijkend onderzoek aan de
	ECDC en werkt samen met WHO. ECDC en WHO gebruikt de gegevens voor de bestrijding van C19 op Europees of Internationaal niveau.
Derden	Het samenwerkingsverband Influenzanet heeft belang bij het uitvoeren van Internationaal vergelijkend onderzoek. Tevens hebben andere Influenzanet partners voordeel van ontwikkelingen in het platform uitgevoerd door het RIVM. Net als het RIVM profiteert van verbeteringen door anderen.

7. Verwerkingslocaties

Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden. Beschrijf het doorgiftemechanisme (bv. adequaatheidsbesluit) dat van toepassing is wanneer verwerkingslocaties buiten de Europese Economische Ruimte bevinden. Voeg aanvullende informatie toe in het tekstveld.

Zie deel III van het Rijksmodel DPIA voor meer informatie over de doorgiftemechanismen.

De analyse van de gegevens in het kader van dit onderzoek vindt plaats door onderzoekers van het RIVM. Het technisch applicatiebeheer van RIVM Infectieradar (inclusief de software) ligt bij het RIVM, meer specifiek bij de afdeling Applicatie en Functionaliteiten Management. Zij beheert ook de onderzoekersaccounts in RIVM Infectieradar. Het beheer van de vragenlijst-templates en berichtentemplates ligt bij de afdeling EPI.

RIVM Infectieradar wordt gehost bij SSC-Campus (onderdeel van RIVM) en de huisvesting van de systemen vindt plaats bij het Rijksoverheid Datacenter Equinix. Het onderhoud en de technische doorontwikkeling van RIVM Infectieradar wordt uitgevoerd door Coneno. Deze doorontwikkeling en onderhoud staat los van de in productie zijnde RIVM Infectieradar. Doorontwikkeling gaat over het ontwikkelen van nieuwe functionaliteit (bijvoorbeeld een verbeterde authenticatie en autorisatie voor onderzoekers) die als software beschikbaar komt voor het RIVM, waarna het RIVM deze zelf installeert. Het onderhoud gaat over het aanbieden van nieuwe versies en patches, zodat de software up-to-date blijft. RIVM voert deze nieuwe versies zelf door, en Coneno heeft hiervoor geen toegang tot de systemen van het RIVM nodig.

Alle verwerkingen in het kader van deze PIA vinden plaats binnen de EER.

---

8. Techniek en methode van gegevensverwerking

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

Voor een uitgebreide beschrijving van de technische middelen voor de persoonsverwerking, en met name de technische functionaliteit van de pseudonimisatie en dataopslag (inclusief het gebruik hatching, versleuteling en dataopslag) verwijzen we naar de systeemdecompositie v6 en de PSA RIVM Infectieradar (**zie Bijlage 1 en Bijlage 2**).

Er is **geen** sprake van automatische besluitvorming, profilering of big data analyse zoals bedoeld in de AVG.

Binnen het onderzoek (maar niet binnen de software) wordt gebruik gemaakt van moderne statistische methoden en technieken om de onderzoeksgegevens te onderzoeken en te analyseren. Sommige van die technieken vallen in de categorie "machine learning". Dit wil zeggen dat voor sommige analytische problemen we de computer een oplossing laten zoeken binnen de data. Een voorbeeld hiervan is om binnen de onderzoeksgegevens van alle gebruikers de computer een casus definitie te laten opstellen voor een influenza-infectie. Dit is een noodzakelijke stap in het uitvoeren van onderzoek. Ook in het kader van het Europese onderzoek binnen Influenzanet wordt op basis van deze methoden en technieken onderzoek uitgevoerd. In beide gevallen leiden de uitkomsten en resultaten van dit onderzoek op geen enkele wijze tot uitkomsten die gevolgen hebben voor de deelnemers. Dit komt omdat de deelnemer input levert middels de vragenlijsten, maar de resultaten van het onderzoek niet teruggekoppeld worden of hier gevolgen voor de deelnemer aan worden verbonden.

---

9. Juridisch en beleidsmatig kader

Benoem alle wet- en regelgeving en beleid met mogelijke gevolgen voor de voorgenomen gegevensverwerkingen. De AVG en de Richtlijn[1] hoeven niet genoemd te worden. Voeg aanvullende informatie toe in het tekstveld.

- WMO (Wet medisch-wetenschappelijk onderzoek met mensen)
- De METC van het UMC Utrecht heeft een niet-WMO verklaring afgegeven voor dit onderzoek (METC-protocolnummer 13-673/C).
- Wet op het RIVM
- Archiefwet
- Selectielijst RIVM 2004 – (Staatscourant Nr. 20886, april 2017)
- Nederlandse gedragscode wetenschapsbeoefening
- ICT-Beveiligingsrichtlijnen voor Webapplicaties, NCSC
- Quickscan BIO

---

10. Bewaartermijnen

Bepaal de bewaartermijnen van de persoonsgegevens aan de hand van de gegevensverwerkingen en de verwerkingsdoeleinden. Motiveer waarom deze bewaartermijnen niet langer zijn dan strikt noodzakelijk ten opzichte van de verwerkingsdoeleinden. Beschrijf wie toeziet op de bewaartermijn en de mogelijke vernietiging of archivering aan het einde van de bewaartermijn. Voeg aanvullende informatie toe in het tekstveld.

De onderzoeksgegevens worden in principe 10 jaar bewaard na archivering van de database. Dit is op grond van proces 4.5 de huidige selectielijst. Voorafgaand aan archivering wordt bepaald welke termijn gekozen wordt voor de persoonsgegevens, hierbij kan beroep worden gedaan op een uitzondering, pas na anonimisering van de onderzoeksgegevens. Het bepalen van deze termijn is om te evalueren of de persoonsgegevens nog nodig zijn in de toekomst, wat past bij de taak van algemeen belang. Na het verstrijken van de 10 jaar wordt er een belangenafweging gemaakt of het nog noodzakelijk is dat de gegevens bewaard blijven.[1]

Accountgegevens (van volledig geregistreerde deelnemers)
Accountgegevens worden beheerd binnen de applicatie. Deze informatie wordt bewaard totdat de deelnemer zich afmeld, of tot twee jaar na de laatste activiteit van deze deelnemer. Dit proces van verwijdering van accountgegevens wordt automatisch ingeregeld binnen de applicatie. Met de termijn van twee jaar heeft een inactieve deelnemer de mogelijkheid op een later tijdstip opnieuw vragenlijsten in te vullen. Op die manier kan de deelnemer ook tijdens de actieve periode benaderd worden voor het invullen van de vragenlijsten, zonder dat er vanuit het onderzoek opnieuw stappen genomen moeten worden nieuwe deelnemers te vinden. De termijn van twee jaar is toegepast omdat deelnemers misschien passief zijn voor 1 seizoen. Door het termijn op 2 jaar te zetten kunnen deelnemers 1 seizoen overslaan en toch voor een daarop volgend seizoen worden uitgenodigd. En met een langere termijn kan worden beschikt over een grotere pool van voormalig deelnemers om snel uit te nodigen in het geval dat nodig is; bijvoorbeeld in het geval van een dreigende pandemie.
De deelnemer heeft een duidelijke opt-out voor deelname – namelijk mogelijkheid afmelden onderzoek in de persoonlijke instellingen.
Dit houdt onder andere in dat deelnemer account wordt verwijderd. Daarnaast heeft deelnemer de mogelijkheid om zowel de wekelijkse reminder, als verdere e-mails aan alle deelnemers uit te schakelen.

Accountgegevens (van niet volledig geregistreerde deelnemers)
Potentiële deelnemers die zich opgeven maar niet hun e-mail verifiëren hebben het administratieproces niet voltooid. Dit zijn niet volledig geregistreerde deelnemers. Na 24 uur vervalt de verificatielink en moeten ze zich opnieuw registreren als ze toch willen mee doen. Na 36 uur worden daadwerkelijk hun emailadres en wachtwoord automatisch verwijderd uit de database.

Loggegevens
De loggegeven worden bewaard voor 6 maanden, conform de BIO

---

[1] Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

B. Beoordeling rechtmatigheid gegevensverwerkingen

11. Rechtsgrond

Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.

Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd. Iedere rechtsgrond moet aan bepaalde voorwaarden voldoen, voeg in de toelichting op de rechtsgrond toe hoe aan deze voorwaarden wordt voldaan. Voeg aanvullende informatie toe in het tekstveld.

De grondslag(en) voor de verwerkingen zijn:

- Geïnformeerde toestemming. De deelnemers maken in het begin van de wervingsfase van het onderzoek vrijblijvend en vrijelijk de keuze of zij wel of niet toestemming willen geven voor de deelname aan het onderzoek. De deelnemers kunnen vrijelijk kiezen om niet deel te nemen en deelnemers kunnen vrijelijk kiezen om hun deelname te stoppen.
- Algemeen belang. Grondslag uit artikel 6 AVG: Artikel 6 lid 1 sub e AVG: taak van algemeen belang, die zich o.a. manifesteert in artikel 3 lid 1 Wet op het RIVM.

---

12. Bijzondere persoonsgegevens

Het verwerken van bijzondere of strafrechtelijke persoonsgegevens is in principe verboden. Verwerking is pas mogelijk wanneer een uitzonderingsgrond van toepassing is. Beoordeel of een van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een nationaal identificatienummer, beoordeel of dit is toegestaan.

De verwerking is noodzakelijk voor redenen van algemeen belang op het gebied van de volksgezondheid. Met dit onderzoek wordt inzicht verkregen in het verloop van Long Covid. Dit onderzoek kan niet worden uitgevoerd zonder dat er bijzondere gegevens van deelnemers worden verwerkt.

Voor het doel van het onderzoek is de verwerking van persoonsgegevens noodzakelijk. Onder deze persoonsgegevens vallen tevens bijzondere persoonsgegevens, namelijk gegevens over gezondheid waarvoor in beginsel een verbod op verwerking geldt.

Op de verwerkingen in het kader van dit onderzoek is de uitzondering ex artikel 9, tweede lid onder i van de AVG van toepassing. Er is sprake van:
- een grond in Unierecht of lidstatelijk recht (artikel 23 sub a Uitvoeringswet AVG in relatie met EU Besluit EU/1082/2013 art. 6 jo art. 2, artikel 3 Wet op het RIVM en artikel 6c Wpg);
- waarin passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van de betrokkene (de pseudonimiseringsplicht ex artikel 6c.3 Wpg)

---

13. Doelbinding

Als de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld. Voeg in het tekstveld de verenigbaarheidstoets en aanvullende informatie toe.

De persoonsgegevens worden verzameld voor de doeleinden van deze studie, zoals beschreven in onderdeel 4 van deze PIA. Daarbij is het mogelijk dat gegevens van deelnemers die via het PIENTER onderzoek zijn uitgenodigd en deelnemen, op verzoek van het PIENTER team (aan het Infectieradar team) verstrekt worden (door het Infectieradar team) aan het PIENTER team. Voor deze verstrekking is voorafgaand aan deelname aan Infectieradar duidelijk uitgelegd aan de deelnemer van de Pienter studie dat zijn/haar onderzoeksgegevens binnen Infectieradar gedeeld kunnen worden met de Pienter studie als de Pienter studie hier om vraagt (en niet andersom – Pienter data met Infectieradar) . Verder kunnen de onderzoeksgegevens ook gebruik worden in het kader van Europees onderzoek via Influenzanet. Betrokkenen worden hierover geïnformeerd en de gegevens worden hiervoor verder gepseudonimiseerd (leeftijdsgroep ipv leeftijd en regio ipv PC4). De doeleinden van dit Europese onderzoek zijn verenigbaar met het doel van deze studie: betrokken worden hierover geïnformeerd, de doeleinden van de Europese studie zijn hetzelfde als van deze studie, de risico's voor betrokkenen zijn minimaal (kans op (indirecte) herleidbaarheid wordt verder verkleind door aanvullende pseudonimisering, en tot slot heeft ook die verwerking geen directe of indirecte gevolgen voor de deelnemers.

---

14. Noodzaak en evenredigheid

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

a. Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?

b. Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, worden verwezenlijkt?

Er is een focus op het aantal mensen met symptomen van een infectie, de impact van deze infectie op het leven van de patiënt, de zorgvraag door de patiënt, en hoe lang het duurt voordat een patiënt daadwerkelijk zorg vraagt na het begin van de eerste symptomen (reporting delay). De zorgvraag en reporting delay zijn essentiële parameters om gegevens van andere surveillance systemen juist te interpreteren.

Om een juiste interpretatie van de verzamelde gegevens binnen infectieradar te waarborgen is het essentieel om te weten hoe de bevolkingssamenstelling in het panel overeenkomt met de Nederlandse bevolking. Ook is het belangrijk om analyses te kunnen doen voor relevante subgroepen zoals ouders met kinderen, ouderen, diabetes patiënten en gevaccineerden. Deze subgroepen worden vastgesteld op basis van en zijn beperkt tot de gegevens die verstrekt zijn via de vragenlijsten.

De huidige gegevensverwerking zijn proportioneel omdat:

1. De verwerking van de gegevens essentieel is voor het uitvoeren van dit onderzoek van RIVM Infectieradar om zo bij te dragen aan de doelstellingen van dit onderzoek. De gegevens worden door deelnemers op basis van geïnformeerde toestemming verstrekt, nadat zij hierover conform de voorwaarden in de AVG hierover geïnformeerd zijn. De gegevens worden door de deelnemers zelf verstrekt en de deelnemers zijn geïnformeerd over de relevantie van de gevraagde gegevens. De deelnemers zijn niet verplicht om de gegevens te verstrekken, maar hebben de mogelijkheid om aan te geven dat zij bepaalde gegevens niet willen verstrekken.;
2. Er slechts gegevens verzameld worden die noodzakelijk zijn voor de uitvoering van het onderzoek en haar doelstellingen.
3. Vanwege de persoonlijke aard van de gegevens, zoals symptomen, is er geen andere manier om zo de hieraan verbonden ernstige gevolgen voor de volksgezondheid en staat van de Nederlandse economie te beperken, en er geen andere manier is om aan voldoende van dit soort gegevens te komen.

Daarnaast is bij de gegevensverwerking sprake van subsidiariteit, omdat:

1. Zonder deze gegevens kunnen de doelstellingen niet bereikt worden;
2. Deze gegevens niet op een andere, minder ingrijpende wijze verzameld kunnen worden. De reden hiervoor is dat de wekelijkse vragenlijst diverse gegevens in kaart brengt, die niet in deze mate en niet wekelijks bij bijvoorbeeld een zorgverlener worden geregistreerd. Indien dat wel het geval zou zijn, ook dan geldt als voorwaarde dat de deelnemer hiervoor zijn uitdrukkelijke toestemming moet geven voordat die gegevens beschikbaar kunnen worden gesteld.

Geconcludeerd kan worden dat de overwerkingen in het kader van dit onderzoek beperkt zijn tot persoonsgegevens die noodzakelijk zijn voor de uitvoering van het onderzoek, de belangen van deelnemers niet onevenredig schaden en niet op een minder ingrijpende wijze verkregen kunnen worden. In hoofdstuk 2 is meer te lezen over de noodzakelijkheid per persoonsgegeven die verwerkt word.

15. Rechten van de betrokkene

Beschrijf de procedure waarmee invulling wordt gegeven aan de rechten van de betrokkenen en welke partij verantwoordelijk is voor de uitvoering van de procedure. Als de rechten van de betrokkene worden beperkt, beschrijf op grond van welke wettelijke uitzondering dat is toegestaan.

De rechten van de betrokkenen zijn o.a. belegd in de AVG. Daarnaast kent de Uitvoeringswet van de AVG (UAVG) een aantal uitzonderingen op deze rechten ingeval van wetenschappelijk onderzoek.

De rechten van de betrokkenen zijn o.a. belegd in de AVG en de Uitvoeringswet van de AVG (UAVG).

Wanneer een betrokkene zijn rechten wil uitvoeren, zal de hoofdonderzoeker een goede afweging maken t.a.v. het honoreren van een verzoek. Het RIVM streeft altijd naar een zorgvuldige afweging tussen de belangen van de betrokkene, het algemeen belang en het wetenschappelijke belang. In beginsel zal de hoofdonderzoeker bepalen wat in redelijkheid is uit te voeren en hoe de rechten en vrijheden van de betrokkenen zo goed mogelijk worden gewaarborgd. De hoofdonderzoeker wordt geacht het beste overzicht te hebben over de verwerkingen binnen de project en hier ook verantwoordelijkheid over draagt. Hieronder volgt een toelichting per recht.

Recht op duidelijke informatie over wat het RIVM met de gegevens doet (art.13 en 14 AVG)

De deelnemers hebben voorafgaand aan de deelname aan de project een privacyverklaring en een toestemmingsverklaring ontvangen en zij hebben de gelegenheid gekregen hierover na te denken en vragen te stellen. In deze privacyverklaring staat ook informatie over de verwerking van persoonsgegevens, inclusief de rechten van de betrokkene. Daarbij wordt verwezen naar de privacy statement en op de website van het RIVM. Daarnaast wordt er wekelijks gepubliceerd, in geaggregeerde vorm, op de resultaten pagina van het onderzoek. Resultaten worden ook openbaar gemaakt via wetenschappelijke publicaties.

Stoppen met het onderzoek/intrekken toestemming deelname (art. 7 AVG)

Deelname aan het project vindt plaats op grond van toestemming, maar vindt de verwerking van persoonsgegevens plaats op grond van 'taak van algemeen belang' (zie ook hoofdstuk 11). In eerste instantie is de deelnemers om toestemming gevraagd op grond van de AVG. Later is deze grondslag gewijzigd en is dit aan de deelnemers kenbaar gemaakt op

Toch wordt v.w.b. de rechten van betrokkenen aangesloten op het AVG-regime van de grondslag 'toestemming'. Er is een directe afhankelijkheidsrelatie met de deelnemers, en worden de wensen van deelnemers voor zover mogelijk gerespecteerd.

De deelnemer kan zich op elk moment bedenken en stoppen met de deelname aan het onderzoek, zoals ook vermeld in de privacyverklaring en toestemmingsverklaring. Indien de deelnemer stopt, worden er geen nieuwe gegevens meer verzameld bij de deelnemer. Alle persoonlijke details van de deelnemers worden dan verwijderd, dus zijn dan niet meer direct te herleiden aan een persoon. De reeds verzamelde gepseudonimiseerde gegevens blijven aanwezig voor wetenschappelijke analyse.

Indien de deelnemer de toestemming intrekt, dan worden de persoonlijke gegevens verwijderd, maar de reeds gedeelde onderzoeksgegevens blijven bewaard en worden verder verwerkt voor de wetenschappelijke analyse en voor archivering. De gegevens zijn namelijk nu gepseudonimiseerd, maar als de accountgegevens worden verwijderd is het technisch onmogelijk om de gegevens opnieuw te verbinden aan de accountgegevens.

Recht op inzage (art 15 AVG)

De betrokken heeft recht op inzage. Bij een verzoek tot inzage zal beoordeeld moeten worden welke data kan worden teruggekoppeld, zoals de gegevens die verzameld zijn voor het uitvoeren van de project. Nadat de project is beëindigd, wordt gestart met het klaarmaken van de gegevens voor 'archivering'. Op dat moment begint de vernietiging van directe persoonsgegevens en zijn resterende direct herleidbare persoonsgegevens niet meer aanwezig. Vanaf dat moment is het verzoek tot inzage niet meer mogelijk.

Recht op rectificatie en aanvulling (art. 16)

Indien een deelnemer of teamlid aangeeft dat informatie niet correct is, wordt de data aangepast tenzij dit niet mogelijk is. Wijzigingen in de projectdatabase worden gelogd.

Recht op vergetelheid/gegevenswissing (art. 17 AVG)

Deelname aan het project vindt plaats op grond van toestemming, maar vindt de verwerking van persoonsgegevens plaats op grond van 'taak van algemeen belang'. Strikt genomen hoeft dit verzoek van de betrokkene (verzoek tot gegevenswissing) niet te worden gehonoreerd.

Indien een betrokkene een beroep doet op het Recht op vergetelheid, wordt dit in beginsel gehonoreerd voor de persoonsgegevens binnen het Infectieradar portaal en GLEAN (e-mail, voornaam/achternaam, adres, telefoonnummer). De gepseudonimiseerde gegevens die al zijn verzameld blijven bewaard, omdat deze dan al gebruikt en benodigd zijn voor het onderzoek dat al is uitgevoerd.

Recht op beperking van de verwerking (art. 18 AVG)

Indien een betrokkene een beroep doet op het Recht op beperking van de verwerking, wordt dit in beginsel gehonoreerd.

Kennisgevingsplicht (art. 19 AVG)

Indien een betrokkene een beroep doet op het recht zoals vermeld in dit artikel, wordt dit in beginsel gehonoreerd.

Recht op overdraagbaarheid van gegevens (art. 20 AVG)

De uitvoering van dit recht wordt per keer beoordeeld. Het kan zijn dat een deelnemer aan meerdere onderzoeken wenst deel te nemen en om overdracht van de gegevens vraagt. In beginsel wordt het verzoek gehonoreerd.

Recht op bezwaar te maken tegen de gegevensverwerking (art. 21 AVG)

Deelname aan het project vindt plaats op grond van toestemming, maar vindt de verwerking van persoonsgegevens plaats op grond van 'taak van algemeen belang' (zie hoofdstuk 11). Strikt genomen hoeft dit verzoek van de betrokkene (Recht op bezwaar te maken tegen de gegevensverwerking) niet te worden gehonoreerd.

Toch wordt v.w.b. de rechten van betrokkenen aangesloten op het AVG-regime van de grondslag 'toestemming'. Er is een directe afhankelijkheidsrelatie met de deelnemers, en worden de wensen van deelnemers voor zover mogelijk gerespecteerd.

Indien een betrokkene een beroep doet op het recht zoals vermeld in dit artikel, wordt dit in beginsel gehonoreerd.

Recht met betrekking tot geautomatiseerde besluitvorming en profilering (art. 22 AVG)

Er wordt geen gebruik gemaakt van geautomatiseerde, gebaseerde besluitvorming, waaronder profilering.

C. Beschrijving en beoordeling risico's voor betrokkenen

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de voorgenomen gegevensverwerkingen

16.Risico's

De risico's voor de betrokkene zijn beschreven in de risicoanalyse: zie RIVM Risicoanalyse – Influenzanet 2_0 ISO27005 -20200830.

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

Risico 1: Onrechtmatig gebruik door onbedoelde herleidbaarheid

Impact

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

NB De impact op de rechten en vrijheden van betrokkenen kan sterk variëren, afhankelijk van de gegeven antwoorden/beschreven situatie.

Kans

RIVM treft verschillende maatregelen om spontane en onbedoelde herleiding te voorkomen (zie hierna). De kans dat er negatieve gevolgen zullen optreden kan daarom als klein worden beschouwd.

De onderzoeksgegevens zijn gepseudonimiseerd. De accountgegevens kunnen herleidbaar zijn (op basis van naamgebruik in het e-mailadres), maar beide type gegevens worden gescheiden opgeslagen in gescheiden databases en zijn door onderzoekers niet aan elkaar te koppelen. Daarnaast zijn de wachtwoorden encrypted. Koppeling van gegevens uit beide databases is slechts mogelijk met een sleutel die gehased en encrypted is (MD5-hash en AES-encryptie in CTR-mode). Hierdoor zijn de gegevens op een wijze gepseudonimiseerd dat (indirecte) herleidbaarheid zonder aanvullende gegevens in redelijkheid niet mogelijk is.

Risico 2: Datalekken

Impact

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

Kans

De kans op een datalek is klein, omdat de account- en onderzoeksgegevens gescheiden zijn opgeslagen en zonder de sleutel niet aan elkaar gekoppeld kunnen worden. Daarbij speelt mee dat deze sleutel gehashed en encrypted is. Ook zijn de onderzoeksgegevens gepseudonimiseerd, waardoor bij een eventueel datalek de gegevens niet in redelijkheid herleidbaar zijn tot een individuele deelnemer.

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

Risico 3: Function creep

Met behulp van de vragenlijsten vullen deelnemers diverse persoonsgegevens in. Een deel hiervan betreft bijzondere gegevens. Vanwege de aard van de gegevens, en de mate waarin deze gegevens verzameld worden, kunnen de gegevens mogelijk ook voor andere doelen bruikbaar zijn en daardoor onbedoelde functies gaan vervullen.

Impact

RIVM verwerkt vele soorten gegevens in verschillende typen onderzoeken. De onderzoeksresultaten worden voornamelijk gebruikt om de rijksoverheid of zorgverleners te adviseren omtrent publieke gezondheid en gerelateerd beleid. Verwerkingen hebben (bijna) nooit tot doel om directe impact te hebben op individuele betrokkenen, ook hier niet. Als het RIVM zou besluiten om gegevens verder te verwerken voor onderzoeken (zelfs als dat onrechtmatig zou gebeuren) zou de impact op betrokkenen niet groot zijn. De kans bestaat wel dat betrokkenen een gevoel van verlies van controle over hun gegevens ervaren (zie Risico 4).

Kans

De kans op onrechtmatige verdere verwerking van persoonsgegevens is zeer klein; RIVM voert voor onderzoeken DPIA's uit en is zich zeer bewust van haar maatschappelijke rol. De kans dat persoonsgegevens verder worden verwerkt op een onrechtmatige wijze is lastig in te schatten, tenzij expliciet beleid vastlegt dat dat niet gaat gebeuren.

Risico 4: Verlies controle over persoonsgegevens

Betrokkenen moeten in principe voorafgaand aan enige verwerking weten wat er met hun persoonsgegevens gebeurt. Hiervoor is het ook van belang dat betrokkenen duidelijk weten welke rechten zij kunnen uitoefenen, en op welke wijze zij dit kunnen doen. Deze rechten zijn niet absoluut, maar dienen wel te allen tijde effectief te zijn.

Impact

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

Kans

De kans dat dit risico zich voordoet is laag tot gemiddeld. De studie bevat duidelijke en afgebakende doelstellingen, waarbij eventuele verstrekking (en de bijbehorende voorwaarden) aan derden is beschreven. Verder kunnen deelnemers via het persoonlijke account van LongCOVID onderzoek hun persoonsgegevens niet inzien, vanwege het ontbreken van 2MFA.

D. Beschrijving voorgenomen maatregelen

17.Maatregelen

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

Er zijn door het RIVM verschillende maatregelen genomen om de risico's voor betrokkenen te beperken.

Hieronder is per risico beschreven welke maatregelen kunnen helpen de kans en impact van de risico's te verkleinen naar een acceptabel niveau. Input voor de maatregelen is mede gebaseerd op de uitgevoerde IB Risicoanalyse (zie Bijlage 6:Privacy Risicoanalyse Infectieradar).

De maatregelen geven duidelijke richting en concrete houvast, maar zijn geen kant en klare procesbeschrijving. Dat laat ruimte de maatregelen te implementeren op een wijze die het beste aansluit bij het de risico-acceptatie van het RIVM.

Maatregelen: Onrechtmatig gebruik door onbedoelde herleidbaarheid

Gerealiseerd:

1. Vercijferde verbinding van uit de web-client met de APIs. TLS 1.2 of hoger;
2. Ingeperkte database-rechten vanuit de participant API;
3. Bij de verwerking van persoonsgegevens wordt een onderscheid gemaakt tussen accountgegevens (email en wachtwoord) en de onderzoeksgegevens (persoonsgegevens die worden verzameld in de vragenlijsten). Accountgegevens en onderzoekgegevens worden gescheiden opgeslagen in verschillende databases die staan in verschillende microservices.
4. Herleidbaarheid van gegevens wordt zoveel mogelijk voorkomen door de deelnemers niet te vragen naar naam, adres, volledige geboortedatum;
5. Accountgegevens en onderzoekgegevens zijn alleen gelinkt met een unieke, versleutelde studie specifieke ID **(MD5-hash en AES-encryptie in CTR-mode zie de Bijlage 1: Project Start Architectuur (PSA) RIVM Infectieradar v1.6 voor gedetailleerde informatie);**
6. Onderzoeksgegevens worden gepseudonimiseerd verwerkt en opgeslagen in de database;
7. Onderzoekers kunnen alleen gepseudonimiseerde onderzoeksgegevens downloaden;
8. Onderzoekers mogen alleen rapporteren op geaggregeerde onderzoeksgegevens (waarbij geldt: N>5);
9. Onderzoekers hebben géén toegang tot de database met accountgegevens;
10. Onderzoekers hebben géén toegang tot de database met mobiele telefoonnummers;
11. Mobiele telefoonnummers worden opgeslagen in een andere database, met een ander ID, en zijn dus niet herleidbaar naar onderzoeksgegevens.
12. Gepseudonimiseerde data die worden gedeeld met eventuele onderzoekspartners zijn bewerkt om indirecte herleidbaarheid verder uit te sluiten. De postcode wordt vervangen door regio (NUTS3 of lager) en de leeftijd wordt vervangen door een leeftijdscategorie;
13. Toegang tot de study-API services buiten het RIVM-netwerk is geblokkeerd;
14. Logging van toegang tot en wijziging van persoonsgegevens in de applicatie en database;

Maatregelen: Function creep

Gerealiseerd:

15. Vastgelegd op grond van welke voorwaarden onderzoeksgegevens voor andere doeleinden gebruikt mogen worden;
16. De studie heeft een duidelijk afgebakend doel waarin het gebruik en het delen van de onderzoeksgegevens – zover relevant – is beschreven;

Maatregelen: Datalekken

Gerealiseerd:

17. Back-end alleen te benaderen via RIVM account en 2F en 4 ogen principe
18. Account- en onderzoeksgegevens worden in twee separate databases opgeslagen;
19. Accountgegevens en onderzoekgegevens zijn alleen gelinkt met een unieke, versleutelde studie specifieke ID (zie de Bijlage 1: Project Start Architectuur (PSA) RIVM Infectieradar v1.6 voor gedetailleerde informatie);
20. Onderzoeksgegevens worden gepseudonimiseerd verwerkt en opgeslagen in de database;
21. De software van RIVM draait op servers van het RIVM zonder externe partijen (dus geen problemen met datatransfer en toegang van derden tot de back-end);
22. RIVM maakt gebruik van betrouwbare servers (ISO 27001 gecertificeerd data center) in Amsterdam van Equinix.
23. Toegang tot het RIVM gebouw en het Amsterdamse datacenter is alleen via fysieke en technische beveiligde toegang mogelijk;
24. Er wordt geen technische informatie getoond over de (werking van) applicatie-software en het onderliggend platform;
25. Maatregelen tegen cross-site request forgery; toepassen content security policy-header; 26. E-mails aan deelnemers worden door de software geautomatiseerd verstuurd, waarbij geldt:

a. De links in de uitnodigingsmail voor vragenlijsten en account verificatie hebben beperkte geldigheidsduur;
b. Er wordt gebruik gemaakt van niet-voorspelbare codes in de links;
c. Authenticatie van deelnemers tijdens inloggen op www.Rivm.nl/longcovidonderzoek ;
d. Controle op uitgifte van vragenformulieren d.m.v. tokens;

27. Uitvoeren van pentest door onafhankelijke partij in Augustus/September 2020 (zie Bijlage 10: Documentatie pentest en code-review) in Nederland; en uitvoeren van pentest door een onafhankelijke partij voor dezelfde software in België in Februari 2021;
28. Deelnemers hebben geen toegang tot vorige vragenlijsten of gegevens die ze eerder hebben aangeleverd.

Maatregelen: Verlies van controle van persoonsgegevens

Gerealiseerd:

29. Privacyverklaring met relevante informatie van de meest actuele versie van de www.rivm.nl/longcovidonderzoek, waaronder:

a. Welke persoonsgegevens worden verzameld, de doeleinden voor de verzameling en de betreffende rechtsgrond voor de verwerking;
b. Informatie over de verdere verwerking, door welke partijen voor welke doeleinden;
c. Informatie over de (inperking) van rechten van betrokkenen en de wijze waarop zij die rechten kunnen uitoefenen;
d. Toepasselijke bewaartermijn en de reden daarvoor.

30. Toelichting tijdens de aanmelding op heldere wijze toe waarom bepaalde rechten worden beperkt, en op welke wijze bescherming van de persoonsgegevens in dat kader wordt gewaarborgd;
31. Zorg dat binnen het OpenShift platform (waarin beheerders werken) op individueel niveau gelogd kan worden;

32. Verstrekken heldere mogelijkheden om deelname aan het LongCOVID onderzoek te beëindigen
33. Expliciete mogelijkheid om "wil ik niet aangeven" voor de gevoelige velden (geboorte maand/ postcode/klinische risicogroep);
34. Na 1 jaar inactiviteit van het www.rivm.nl/longcovidonderzoek-account worden de accountgegevens verwijderd;
35. Uitvoeren van code-review door een onafhankelijke partij ten behoeve van integriteit, betrouwbaarheid en beschikbaarheid (zie Bijlage 10: Documentatie pentest en code-review);
36. Invoeren van controles in de formulieren;
37. Biedt de gebruiker de mogelijkheid de sessie op eigen initiatief te beëindigen (uitloggen).
38. Zorg dat binnen het OpenShift platform (waarin beheerders werken) op individueel niveau gelogd kan worden;

Maatregelen: Ongeldige toestemming

Gerealiseerd:

39. Toestemmingsverklaring met relevante en overzichtelijke informatie en in heldere en begrijpelijke taal;
40. Het is beschreven in de toestemmingsverklaring welke partijen de onderzoeksgegevens kunnen ontvangen en voor welk doeleinde dit gebeurt;
41. Er is tijdens de aanmelding een toestemmingsverklaring waarin de deelnemer expliciet toestemming verleend voorafgaand aan deelname
42. Een toestemmingsverklaring specifiek voor het LongCOVID onderzoek;

Generieke beveiligingsmaatregelen

Toepassing van diverse technische beveiligingsmaatregelen zoals die binnen het RIVM standaard plaatsvinden, waaronder:

Gerealiseerd:

43. Beperking van het aantal te accepteren API-calls van een bron per tijdseenheid (rate limiting) en van het aantal achtereenvolgende inlogpogingen;
44. Er is een ontwerp- en configuratiedocument dat beschrijft op welke wijze processen worden afgeschermd van bestanden waartoe systeem beheerders geen toegang mogen hebben;
45. De-activatie alle protocollen, services en account op het platform als die niet volgens het ontwerp noodzakelijk zijn;
46. Firewalls;
47. Anti-malware software;
48. Gebruik van Google reCaptcha ter identificatie van menselijke gebruiker bij het aanmaken en inloggen van een account op www.rivm.nl/longcovidonderzoek;
49. Invoeren van controles wat betreft formulieren op de server;
50. Controle op uitgifte van vragenformulieren d.m.v. tokens;
51. Voor alle cookies de flags 'secure' en 'HttpOnly' ingesteld;
52. Anti-DDoS dienst geactiveerd;
53. Plaatsing van de applicatie in het DMZ-netwerk;
54. Servicecontract (SLA) met software leverancier;
55. Wachtwoordbeleid: het wachtwoord van een deelnemer voor het LongCOVID onderzoek moet 8 tekens bevatten en 3 van de volgende 4 criteria; tenminste 1 hoofdletter, tenminste 1 kleine letter, tenminste 1 speciaal teken, tenminste 1 cijfer;
56. Na afronding van de inschrijving kan de deelnemer het wachtwoord en e-mailadres wijzigen;
57. Uitgebreid testtraject voor release (OTAP);
58. Dedicated OpenShift-project voor RIVM Infectieradar platform (incl. Infectieradar en LongCOVID)met beperkt beheer-groep;

59. Toepassen van Unit- Integratie- en End-2-endtesten;
60. Versiebeheer van code in Git;
61. Deployment via scripting en build-server.

Reactie n.a.v. het advies van de 5.1.2e

Advies 1: De grootste verandering ten opzichte van de voorgaande versies van Infectieziekteradar, en hiermee een reductie van de privacyrisico's is dat voor de hosting geen gebruik meer gemaakt wordt van externe partijen. Hiermee blijven de (persoons)gegevens volledig in handen en onder beheer van het RIVM. Het RIVM gebruikt voor de RIVM infectieradar software ontwikkeld door Coneno, een softwarebedrijf gelinkt aan het academische instituut DFKI in Duitsland. De software is volledig en onafhankelijk in beheer van het RIVM is. Uit de DPIA blijkt wel dat Coneno geen enkele toegang tot de in productie zijnde software heeft.

Daar waar het doel eerst enkel het aanpassen van landelijke preventie en mitigatiebeleid crisisbeheersing en om bevolking van informatie te voorzien betrof is het doel van de verwerking verbreed naar (wetenschappelijk) onderzoek in bredere zin. En betreft het doel nu het bestuderen van gezondheidsklachten die kunnen wijzen op infectieziekten, in het kader van onderzoek zoals bepaald in artikel 3 Wet op het RIVM. De 5.1.2e ziet hier geen bezwaren in mede gezien de Wet op het RIVM.

De schematische structuurweergave maakt de gegevensstromen inzichtelijk. In de dataflow Infectieradar versie 3.0 d.d. 3-9-2020 (bijlage 2a) staat weergegeven dat 2 databases voor de verwerking in gebruik zijn te weten, de User DB en de Study DB. Het is echter onduidelijk hoe het versturen van de herinneringsmail plaatsvindt. Wellicht vanuit de massagedb welke in de systeemcompositie RIVM infectieradar v6 (bijlage 2) genoemd wordt. In dit document worden ook de databases massagedb en globaldb aangegeven (zie pg.1 bijlage 2). Het is onduidelijk of zich in deze databases persoonsgegevens bevinden. Advies: Verduidelijk de PIA.

Antwoord 1: In de globaldb staan geen persoonsgegevens, in de messagedb staat het e-mailadres in de log-files. Ook staat hierin welke deelnemers een herinneringsmail hebben gekregen. Ook staat hier een template voor de mail die verstuurd moet worden. De mail wordt uiteindelijk verzonden via de mailserver. Dit is al beschreven in bijlage 2B onder punt 1.1.8.

Advies 2: Grondslag

Als grondslag voor de verwerking wordt uitdrukkelijke toestemming gevraagd. Zoals eerder in het traject voor de opzet van infectieziekteradar aangegeven zijn er mogelijkheden om de verwerking op basis van een wettelijke grondslag te baseren. Als de verwerking noodzakelijk is voor de taak van het RIVM inzake infectieziektebestrijding dat ze deze gegevens ontvangt en verwerkt, dan kan artikel 6c WPG als grondslag dienen. We hebben het dan in AVG termen over artikel 6 onder e een taak van algemeen belang/publieke taak in combinatie met artikel 9, tweede lid onder g, waarbij de grondslag is neergelegd in lid statelijk recht, te weten 6c Wet publieke gezondheid.

Antwoord 2: Infectieradar loopt al vanaf november 2020. Destijds was het regime van het RIVM nog om de grondslag toestemming te gebruiken. Sinds januari 2022 is deze grondslag gewijzigd in Taak van Algemeen belang. Om die reden wordt aan de deelnemers van Infectieradar medegedeeld dat er nu sprake is van een nieuwe grondslag. Deelnemers kunnen hun toestemming nog intrekken binnen afzienbare tijd als zij het hier niet mee eens zijn.

Advies 3: Google reCaptcha

Het gebruik van Google reCaptcha kent inherente risico's voor gegevensbescherming. Aangegeven is dat het gebruik hiervan buiten de scope van de DPIA valt omdat dit als een generieke beveiligingsmaatregel gezien wordt dat los staat van deze studie naar infectieziekten. Echter omdat bij deelname aan het onderzoek altijd gegevens van de betrokkene door Google verzameld en verwerkt worden kan de inzet van Google reChapta niet los van van RIVM Infectieradar gezien worden. Inzet van Google reCaptcha valt dan ook binnen de scope van de PIA. Adreseer welke persoonsgegevens en cookies Google verwerkt. Het transparantiebeginsel vereist dat voldoende informatie wordt verstrekt over de wijze van de (verdere) verwerkingen een dergelijke inzet. Uit oogpunt van risico voor de burger is het ook van groot belang inzichtelijk te maken of deze partijen de beschikking krijgen over persoonsgegevens en welke cookies geplaatst worden.

Ten aanzien van de inzet is het volgende te melden. Bij gebruik van Google reCaptcha worden persoonsgegevens verstrekt aan een derde land met een onvoldoende passend beschermingsniveau. Dit gezien het feit dat volgens het Europese Hof de VS op dit moment de privacyrechten van Europeanen onvoldoende beschermt. Daarnaast speelt ook de Freedom Act een rol dat betekent dat de veiligheidsdiensten in de VS toegang hebben tot de gegevens. Tevens speelt mee dat de inzet waarbij persoonsgegevens van burgers door toedoen van de overheid richting Google gaan reputatieschade voor het ministerie als wel het RIVM met zich mee kan brengen. Advies: Inzet van Google reCaptcha wordt ten zeerste afgeraden en geadviseerd wordt dan ook om alternatieven te onderzoeken.

Antwoord 3: Dit advies wordt niet opgevolgd. Per risicoacceptatie ism informatiebeveiliging is besloten om gebruik te maken van Google reCaptcha (zie hiervoor bijlage 9a, 9b en 9c). Op termijn zal worden overwogen om dit aan te passen.

Advies 4: Bewaartermijnen

- **Aangegeven staat een bewaartermijn van 30 jaar. In de selectielijst 4.5 van het RIVM staat 10 jaar aangegeven. Dit staat niet in verhouding tot elkaar. Hierbij speelt het vraagstuk mee in hoeverre bij gegevens zonder identifiër en met aanpassing van postcode en leeftijdscategorie er nog sprake is van (in)direct herleidbare persoonsgegevens. Aangeraden wordt om een onderzoek naar de kans op indirect herleidbaarheid uit voeren. Advies: Pas in eerste instantie een bewaartermijn van 10 jaar voor de onderzoekgegevens toe en onderzoek in hoeverre de kans op indirect herleidbaarheid plaats kan vinden, dan wel hier sprake is van anonieme gegevens. En pas hierop eventueel de bewaartermijn op aan.**

Antwoord 4:

Dit is aangepast naar 10 jaar. De onderzoeksgegevensworden in principe 10 jaar bewaard na archivering van de database. Dit is gebaseerd op proces 4.5. van de huidige selectielijst, namelijk Het (periodiek) verzamelen en verwerken van gegevens op het gebied van volksgezondheid en milieu, ten behoeve van onderzoek en monitoring. Dit is aangepast in de DPIA

Advies 5: Het is onduidelijk welke persoonsgegevens in de logbestanden verwerkt worden en welke bewaartermijnen hieraan gesteld worden. Advies: Neem de bewaartermijnen van de persoonsgegevens die zich in de logbestanden in de DPIA op.

Antwoord 5: De logbestanden worden 6 maanden bewaard. Dit is toegevoegd aan hoofdstuk 10 bewaartermijnen.

Advies 6: Datalekken

Het is onduidelijk of het eerdere risico waarop in juni jl. een datalek heeft plaatsgevonden in maatregelen is ondervangen en een dergelijk datalek niet nog eens kan plaatsvinden. Advies: Pas de PIA hierop aan.

Antwoord 6: Dit risico is er nog steeds. Echter de kans dat het plaats vind is vele malen kleiner – bijna 0:

a) Volledig andere software – datalek was met formdesk, dit is andere software

b) De link is niet gekoppeld aan een vragenlijst, maar aan de applicatie. Dus men kan niet in een half ingevulde vragenlijst komen.

c) Als mensen op de link klikken wordt er eerst gevraagd om een wachtwoord (dubbele beveiliging)

d) Vele malen complexere link – dus niet logisch te raden zoals bij het lek.

e) De link is technisch niet een link – maar een token, waar actief op wordt beheerd.

f) Veel betere database structuur – gescheiden databases met versleutelde IDs. Dus geen naam of e-mail gelinkt aan de vragenlijst maar een complex ID.

g) Er wordt geen data gedeeld in de applicatie.

Bovenstaande is getest in een pentest EN codereview.

Advies 7: Rechten betrokkene

- **Er worden meerdere onderbouwingen aangegeven waarom het recht op vergetelheid en beperkingen van het recht op bezwaar niet van toepassing zouden zijn. Hierbij wordt ook opgevoerd als de verwerking nodig is om redenen van algemeen belang op het gebied van volksgezondheid; als wel als de verwerking nodig is voor het nakomen van een wettelijke verplichting. Echter dan zal dit ook in lijn met de grondslag waarop de gegevensverwerking gebaseerd is moeten zijn, terwijl in de PIA wordt uitdrukkelijke toestemming als grondslag aangegeven.**
- **Aangegeven staat: *'Als het RIVM persoonsgegevens verwerkt die door het RIVM niet herleidbaar zijn tot een betrokkene, zijn de rechten van betrokkenen niet van toepassing en zal het verzoek worden afgewezen. Dit is overeenkomstig art. 11 AVG. Concreet betekent dit dat dankzij de pseudonimisering van de onderzoeksgegevens in deze studie ervoor zorgt dat de persoonsgegevens in redelijkheid niet herleidbaar zijn. Het vergt onevenredig veel inspanning om de pseudonimisatie van de gegevens terug te draaien zodat ze weer herleidbaar zijn.'* Echter het is onduidelijk hoe dit zich verhoudt met de beschrijving in bijlage 1 bij de PIA de PSA waarin aangegeven staat op welke wijze de link tussen bron bestanden en onderzoeksgegevens te herstellen is. Daarnaast is het RIVM in bezit van het sleutel materiaal en zou dus terug kunnen herleiden naar de brongegevens. Advies: verduidelijk de rechten van de betrokkene en de onderbouwing nader waarom art. 11 AVG in relatie tot een onevenredige inspanning van toepassing zou zijn.**

Antwoord 7: Er wordt meegegaan in dit voorstel. Hoofdstuk 15 is hierop aangepast.

Bijlagen

Bijlage 1: Project Start Architecture (PSA) RIVM Infectieradar

Bijlage 2: Systeemdecompositie RIVM Infectieradar

Bijlage 2a: Intectieradar-flows

Bijlage 2b: Authorisatiematrix

Bijlage 2c: Infectieradar-flows beschrijving

Bijlage 3a: Achtergrondvragenlijst

Bijlage 3b: Wekelijkse vragenlijst

Bijlage 4a: Privacyverklaring RIVM mei 2018

Bijlage 5: Aanvraagformulier risicoacceptatie Bijlage

Bijlage 6: Privacy Risicoanalyse Infectieradar

Bijlage 7: Referentie onderzoek Coneno d.d. 31 augustus 2020

Bijlage 8: Procedure omtrent toegang tot databases

Bijlage 9a: Gebruik van Google reCaptcha

Bijlage 9b: Beslissing reCaptcha

Bijlage 9c: Risico acceptatie akkoord

Bijlage 10: Documentatie pentest en code-review

Procedures

1. Procedure 0 – Procedures Infectieradar
2. Procedure 1 - Procedure Aanmelden Infectieradar
3. Procedure 2 – Procedure Afmelden Infectieradar
4. Procedure 3 - Procedure Aanpassen vragenlijsten Infectieradar
5. Procedure 4 - Procedure Aanpassen applicatie Infectieradar
6. Procedure 5 - Procedure gegevensbeheer Infectieradar
7. Procedure 6 - Procedure email afhandeling Infectieradar
8. Procedure 7 - Procedure Uitoefenen rechten van deelnemers Infectieradar
9. Procedure 8 - Procedure delen publicatie gegevens Infectieradar
10. Procedure 9 - Procedure externe communicatie Infectieradar