Rijksinstituut voor Volksgezondheid
en Milieu
*Ministerie van Volksgezondheid,
Welzijn en Sport*

Stuurgroep Covid-registratie

A. van Leeuwenhoeklaan 9
3721 MA Bilthoven
Postbus 1
3720 BA Bilthoven
www.rivm.nl

KvK Utrecht 30276683

5.1.2e

memo

Analyse FG-advies

Datum
5 januari 2021

Ons kenmerk
DVP_203

Behandeld door
5.1.2e
5.1.2e
5.1.2e

Doel
De FG VWS heeft aan RIVM en VWS advies uitgebracht o.b.v. DPIA CIMS release 1.0, 31 december 2020.

Portefeuillehouder Privacy en voorzitter van de Stuurgroep Registratie heeft gevraagd een analyse maken t.b.v. van de stuurgroep covid-registratie op 5 jan 2021.

De bevinding van de FG (pag.6) luidt: "Als datgene dat in de DPIA verklaard wordt klopt dat de mitigerende maatregelen (inclusief de geconstateerde bevindingen volgend uit de risico-analyse CIMS) ook in werking zijn, zijn de restrisico's klein op het moment van livegang".

FG adviseert:

- dringend om zaken goed vast te leggen zodat wordt aangetoond dat de mitigerende maatregelen daadwerkelijk zijn uitgevoerd. Daarbij wordt gewezen dat de inzet van het register ondanks de korte tijdlijn en de maatschappelijke druk een uiterst zorgvuldige ontwikkeling, opzet en inrichting vereist.
- beter uit te werken waarop aanlevering van de COA gegevens aan VWS/RIVM gebaseerd is.

FG heeft nog enkele vragen zoals:

- In het bijzonder op het gebied van dataminimalisatie, waarom het inladen van de BRP gegevens van de gehele bevolking, ook die van degenen die niet als doelgroep uit het vaccinatiebeleid volgen, worden ingeladen. (pag 6)
- Op welke wijze opvolging van de bevindingen en aanbevelingen van tussenadvies Fg is gegeven (pag 5)

FG heeft enkele verduidelijkingsvragen zoals:

- Onduidelijk zou zijn op welke basis van welke grondslag de zorgverlener (GGD-en) vaccinatiegegegevens aan het RIVM verstrekt. Verduidelijking van

part. 3.1.6 en 3.3. zou uitkomst kunnen bieden. (hierover laat FG zich niet verder uit)
- Noodzakelijkheid van het voor langere tijd onderdeel laten uitmaken van de BRP gegevens in CIMS.
- Verwijderen van cliëntgegevens uit CIMS.
- Diverse verduidelijkingsvragen omtrent processen en procedures (zie onder DPIA H2, paragraaf 2.4, 2.5).
- Diverse verduidelijkingsvragen rondom rollen van betrokken partijen (GGD-en, VWS/RIVM).

Een analyse vanuit privacy compliance perspectief leidt tot de volgende vragen:

1. Kan het advies van de FG VWS en RIVM –"wanneer *datgene dat in de DPIA verklaard wordt klopt dat de mitigerende maatregelen (inclusief de geconstateerde bevindingen volgend uit de risico-analyse CIMS) ook in werking zijn, zijn de restrisico's klein op het moment van livegang"* ondanks de nog niet (geheel) opgevolgde adviezen en openstaande vragen en verduidelijkingsvragen opgevat worden als een positief advies op live gang CIMS release 1.0.
2. Zijn de mitigerende maatregelen zoals onder 1 genoemd, daadwerkelijk getroffen, zodat – wanneer het antwoord op vraag 1, ja is, niets aan een verantwoorde live gang in de weg staat.
3. Welke vrijheid van handelen heeft/ neemt VWS & RIVM ten opzichte van het advies van FG.

Advies: gelet op de gezamenlijkheid VWS & RIVM lijkt het raadzaam om samen met VWS stakeholders te verkennen hoe het advies van FG op te vatten dan wel verduidelijking te vragen ten behoeve van gezamenlijke besluitvorming (VWS en RIVM) op live gang.

In het voorliggende memo wordt het advies en de opmerkingen geanalyseerd op impact op de livegang CIMS.

Het advies van de FG VWS
Het advies is "Leg de zaken goed vast, zodat ook aantoonbaar is dat de mitigerende maatregelen daadwerkelijk zijn uitgevoerd".

Het advies wordt als volgt opgevolgd:
- *Uitvoeringsprocessen worden -zover nog niet gedaan- uitgeschreven en geborgd conform QA-procedures van DVP;*
- *Informatiebeveiligingsrisico's en mitigerende maatregelen zijn uitgeschreven in het IB-risicomanagementregister en geborgd conform IB-procedures van RIVM.*

Opmerkingen van de FG VWS

Datum
5 januari 2021

Scope van de DPIA
Er zijn opmerkingen waarbij de scope aan de orde is (COA (H2 2e bullet), noodzakelijkheid bewaartermijn COA gegevens (2.10 1ste bullet), geboorteland (2.3), inzicht in dichten risico's van derde partijen zoals HIS en Zorgmail (H4 2e bullet).

De opmerkingen zijn als volgt geadresseerd:
- *Het COA is buiten scope van release 1.0.*
- *Het geboorteland is uit de verwerking gehaald o.b.v. DPV_197 Besluitnota verwijderen geboorteland.*
- *De verantwoordelijkheid van RIVM reikt van de verwerkingen m.b.t. CIMS en de koppelvlakken met processen en systemen van ketenpartners. RIVM heeft geen verantwoordelijkheid over de verwerkingen en systemen van de ketenpartners. Inzicht in dichten van risico's van ketenpartners is buiten scope van de DPIA.*

Juridische opmerkingen
Er zijn ook opmerkingen van juridische aard:
- opmerkingen die wellicht door de landsadvocaat beantwoord moeten worden (2.9 (rechtsgrond aanlevering COA gegevens) en 3.1 (rechtsgrond toestemming GGD));
- RIVM GGD rollen en verwerkingsverantwoordelijke (2.5); zie onderhanden P analyse.

Inzake de SFTP-server
Gevraagd wordt naar:
- Doel kopie archief SFTP server, bewaartermijn en toepassing dataminimalisatie (voorstel H2 1ste bullet)?
- Hoe lang staan de gegevens op de SFTP server (2.10 3e bullet)?
- Hoe lang is de bewaartermijn van kopie in het archief op de SFTP (2.10, 4e bullet)?

Bestanden die op de SFTP-server aankomen worden binnen enkele seconden door SmartMove opgepakt en ter verwerking aan de database (niet op de SFTP-server) aangeboden. Na verwerking door de database worden ze in een archive directory (dit is geen archief) gezet. Ook deze archive directory bevindt zich niet op de SFTP-server maar verder in het netwerk van RIVM op het geheugenschijven (NAS: Network Attached Storage). Met de privacy/IB-officer DVP is afgesproken dat de bestanden daar maximaal 2 weken blijven staan.
De backup is een standaard backup conform RIVM-procedures. Deze worden 9 maanden bewaard.
Het BRP-bestand wordt na inlezen in CIMS vernietigd. Dit gebeurt binnen 2 wkn na ontvangst van het bestand.

Proces- en flowcharts

Gevraagd wordt naar:
- Flowcharts gegevensverwerking (2.4);
- Proces en flowcharts Lareb RIVM (2.5 2e bullet);
- Flowcharts algehele gegevensstroom (H4 3e bullet).

De procesbeschrijvingen voor de gegevensverwerking en de datastromen worden -voor zover nog niet gedaan- uitgewerkt conform architectuurprincipes van RIVM, en vastgelegd in de documentatiesystemen bij de CIO Office RIVM. Ook de datamodellen worden -voor zover nog niet gedaan- in deze documentatiesystemen vastgelegd.

Het proces voor gegevensuitwisseling met de Lareb komt er als volgt uit te zien:

1. *Lareb levert wekelijks via een beveiligde mail (protonmail) aan* 5.1.2e *@rivm.nl op maandagmorgen in twee excelbestanden (voor de spontane data en onderzoeksdata) een lijst aan met gegevens. Er is voor de maandagmorgen gekozen omdat er in het weekend nauwelijks gevaccineerd wordt en de data in CIMS dan zo compleet mogelijk is.*
2. *Deze lijsten bevatten een BSN of indien geen BSN bekend NAW gegevens (incl. geboortedatum).*
3. *CIMS Beheer zorgt ervoor dat het rapportageteam de gegevens waarvan het BSN bekend is aanvult met het batchnummer.*
4. *CIMS Beheer stuurt hierna de lijst beveiligd naar het regiokantoor.*
5. *Het regiokantoor zoekt handmatig de batchnummers bij de overige regels en stuurt het bestand beveiligd terug naar CIMS Beheer.*
6. *CIMS Beheer stuurt het bestand beveiligd (uiterlijk vrijdag) terug naar Lareb.*
7. *CIMS Beheer zet een overzicht van deze opvragingen klaar op de SFTP server, zodat Ordina de geraadpleegde cliënten kan markeren als opgevraagd voor Lareb.*

Stap 4 en 5 zou evt. vervangen kunnen worden door het bestand in een map klaar te zetten, waar maar een aantal personen toegang toe hebben. Hier wordt nog naar gekeken.

De flowcharts voor de algehele datastroom worden -voor zover nog niet gedaan- uitgewerkt.

Verwijderen cliëntgegevens

Gevraagd wordt naar:
- Verwijderen cliëntgegevens uit CIMS (2.10 2e bullet).

Gegevens worden op verzoek (telefonisch of via cliëntportaal) verwijderd, gegevensaanlevering uit BRP wordt gestopt, vaccinatiegegevens worden geanonimiseerd.

Anonimiseren gegevens

Gevraagd wordt naar:
- Welk algoritme voor anonimiteit (H4 e bullet)?

In de rapportage tooling wordt data gepseudonimiseerd, niet geanonimiseerd, zodat in geval van medisch incident de persoonsgegevens kunnen worden achterhaald.

Restrisico's Informatiebeveiliging

De volgende opmerkingen zijn gemaakt:

- Om als verwerkingsverantwoordelijke voor livegang een afweging van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen te kunnen maken is het van belang om een beeld van de (rest)risico's te hebben. Dit betekent dat de status van de (mitigerende) maatregelen aantoonbaar inzichtelijke zijn, zodat een beeld van de uiteindelijke privacy risico's ontstaat. De DPIA dient dan ook de voornaamste (rest)risico's te benoemen, zodat de verwerkingsverantwoordelijke deze kan afwegen, waar mogelijk adresseren en eventueel accepteren. In onderliggende DPIA is ten aanzien van restrisico's verklaard dat de geconstateerde restrisico's naar alle waarschijnlijkheid voor 8 januari gemitigeerd zijn inclusief afspraken over een toets op de werking.

De meeste geconstateerde restrisico's zijn voor 8 januari gemitigeerd. De overgebleven restrisico's worden voorgelegd voor acceptatie vóór livegang door het RIVM.

- En tevens is aangegeven dat de bevindingen c.q. aanbevelingen volgend uit de analyses van verschillende externe experts allen zijn opgevolgd of geadresseerd.

Dit geldt ook voor bevindingen c.q. aanbevelingen volgend uit de analyses van de verschillende externe experts.

- De externe analyses betreffen (a) de beoordeling door de Chief Security Privacy Operations van het Programma Digitale ondersteuning, (b) een analyse van Bureau Noordbeek, (c) een analyse van Secura en (d) een audit door de Audit Dienst Rijk (ADR. Op welke wijze opvolging van de bevindingen en aanbevelingen heeft plaatsgevonden staat niet gespecificeerd in de DPIA en is ook niet als bijlage toegevoegd en is hiermee voor mij niet te toetsen. Tevens wordt niet ingegaan hoe met de constateringen uit de risicoanalyse CIMS12 is omgegaan en wat de status hiervan is.

Op reguliere basis wordt een update gemaakt van het risico register. (zie CIMS_Issue_actielijst IB vs 1.53). Met betreffende personen wordt de voortgang van de mitigerende maatregelen en acties besproken en vastgelegd. De meest actuele versie wordt nog nagestuurd aan FG.

- De FG is erg benieuwd hoe onder andere de volgende risico's aangemerkt zijn. Hierbij een reactie daarop:

  - het gebruik van de excel-bestanden (CSV-bestanden).

Vooralsnog wordt geen gebruik gemaakt van Excel. Er zijn afspreken over CSV bestanden. CSV bestanden worden via versleutelde verbindingen verstuurd. De

versleuteling van de data wordt nog nader onderzocht. Er is format controle. Zie ook risico register.

- het beheer van speciale toegangsrechten (systeem- en databasebeheerders) dat onvoldoende beperkt en gecontroleerd bleek te zijn. In de DPIA wordt aangegeven dat het gebruik van de CIMS database door de administrators op persoonsniveau wordt gelogd. Echter in hoeverre vindt ook actieve monitoring plaats?

Monitoring is opgepakt in samenwerking met het Security Operations Center. Use cases worden verder gedefinieerd.

- de data in de CIMS database ten aanzien van versleuteling.

Er vindt standaard versleuteling plaats zowel op de on- en offsite back up. Daarnaast zijn extra maatregelen genomen zoals striktere toegang, logging en monitoring op persoonsniveau, netwerkzonering en mogelijke versleuteling van de primaire database wordt in de nabije toekomst verder onderzocht.

- Het gebruik van de Secure File Transfer Protocol (SFTP) en het emailen van gevoelige informatie.

Er wordt geen gebruik gemaakt van email, wel gebruik van Zorgmail. Maatregelen zijn getroffen naar aanleiding van het onderzoek Secura en ADR op de SFTP server (zie ook risicoregister).

- Voor de FG is het momenteel onduidelijk waaruit blijkt dat de mitigerende maatregelen hebben plaatsgevonden. Haar dringende advies is om voor goede vastlegging te zorgen zodat de mitigatie ook aantoonbaar is, inclusief wat exact gedaan is.

Op dit moment fungeert het risico register voor een vastlegging van de mitigatie en afspraken over audits en scans. Dit wordt na live gang op een structurele manier ingeregeld en belegd.

- Het is voor de FG onduidelijk wat met restrisico (9) – de registratie van cliëntgegevens blijft beperkt tot personen die in het BRP-bestand voorkomen- bedoeld wordt.

COA en Probas zijn geen onderdeel van release 1.0 en derhalve buiten scope.

- Het advies is tevens om uiterst scherp te blijven op datgene dat op het moment van schrijven van de DPIA binnen of buiten scope geplaatst wordt. En op weg naar de livegang toets momenten in te bouwen om te bepalen of datgene dat binnen scope van de alsdan geactualiseerde versie van de DPIA moet zijn ook daadwerkelijk binnen scope is, met specifieke aandacht voor derde partijen.

Het advies wordt ter harte genomen. Er wordt een toets ingepland op de werking van de mitigerenede maatregelen.