Departementaal VERTROUWELIJK.

Bijlage	**Advies Functionaris voor gegevensbescherming VWS DPIA COVID-19 CIMS (automatisch) selecteren en oproepen door het RIVM 'CIMS release 2.0)**
Contactgegevens:	5.1.2e @minvws.nl
Datum advies:	17 februari 2021

Inleiding FG

De functionaris voor gegevensbescherming (hierna: FG) van het ministerie VWS is op grond van het bepaalde in artikel 35, tweede lid, van de Algemene verordening gegevensbescherming (AVG), geraadpleegd over de gegevensbeschermingseffectbeoordeling - GEB, hierna te noemen DPIA over de (voorgenomen) verwerking in het kader van het selecteren en oproepen van burgers voor het vaccinatieprogramma tegen COVID-19 met behulp van het centraal registratiesysteem: het COVID-vaccinatie Informatie- en Monitoringsysteem (hierna: CIMS). Dit advies heeft betrekking op de DPIA Vaccinatieprogramma-COVID-19 CIMS (automatisch) selecteren en oproepen (fase ii) door het RIVM 'CIMS release 2.0, versie onbekend ontvangen 15 februari 2021. In een eerder stadium van de opzet van CIMS is door de FG een advies[1] op de voorgenomen verwerking ten aanzien van de verwerkingen van het centrale vaccinatieregister gegeven.

De AVG legt verantwoordelijkheid bij de organisatie om aan te tonen dat aan de privacyregels is voldaan. Deze verantwoordingsplicht (accountability) houdt in dat de organisatie moet kunnen aantonen dat de verwerkingen aan de regels van de AVG voldoen. Het uitvoeren van een data protection impact assessment (DPIA) voor gegevensverwerkingen met een hoog privacy risico is een verplichte maatregel voor de verantwoordingsplicht van een organisatie. Door te voldoen aan haar verantwoordingsplicht (accountability) levert de organisatie een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy.

Een DPIA is een verplicht hulpmiddel om bij een voorgenomen verwerking van persoonsgegevens, de privacy-risico's (dit wil zeggen de risico's voor de rechten, vrijheden en de effecten voor de betrokkenen) op een gestructureerde en heldere wijze in kaart te brengen en te beoordelen. Zodat op basis hiervan in een vroeg stadium maatregelen getroffen kunnen worden om deze effecten voor betrokkenen te voorkomen of te verkleinen. De DPIA dient de voornaamste (rest)risico's te benoemen, zodat de verwerkingsverantwoordelijke deze kan afwegen, waar mogelijk adresseren en eventueel accepteren.

Advies

Zoals in de DPIA CIMS release 1.0 staat aangegeven: *'Nederland wordt, net als de rest van de wereld, geconfronteerd met de uitbraak van het COVID-19 virus. COVID-19 kan ernstige klachten veroorzaken met als gevolg een acute ziekenhuisopname, een chronisch ziektebeeld, en in het ergste geval, een pijnlijke dood. Momenteel wordt – onder verantwoordelijkheid van de Minister van Volksgezondheid, Welzijn en Sport (hierna: VWS) - een vaccinatieprogramma tegen COVID-19 vastgesteld.[2] Veilige en effectieve vaccins tegen COVID-19 is een essentiële stap in de bestrijding van het coronavirus, en mogelijke beëindiging van de pandemie.*

Het coördineren van de uitvoering, alsmede registratie, bewaking en evaluatie van het vaccin vormt een belangrijk onderdeel van de taak van de Minister van VWS. Deze taak is belegd bij het Rijksinstituut voor Volksgezondheid en Milieu (hierna: RIVM) en het RIVM heeft voornemens om dit te realiseren met behulp van een centraal registratiesysteem: het COVID-vaccinatie Informatie- en Monitoringsysteem (hierna: CIMS).[3]

Een centraal registratiesysteem biedt waarborgen voor een goede en veilige patiëntenzorg en de volksgezondheid. CIMS stelt RIVM onder meer in staat om de uitvoering van het vaccinatieprogramma

[1] Advies Functionaris voor gegevensbescherming VWS DPIA CIMS, d.d. 3 januari 2021
[2] Zie de *Kamerstukken II* 2020/21, 25 295 , nr. 565 en *Kamerstukken II* 2020/21, 25 295 , nr. 745.
[3] *Kamerstukken II* 2020/21, 25 295, nr. 745, paragraaf 6.

te coördineren en te registreren; zicht te hebben en te behouden op het vaccin en – daardoor – tijdig en adequaat te acteren op eventuele incidenten (bijvoorbeeld een kwaliteitsafwijking in een productiebatch) en/of bijwerkingen. Bovendien stelt een centraal registratiesysteem het RIVM in staat om na te gaan hoe het staat met de bestrijding van COVID-19 en in hoeverre het vaccin daaraan bijdraagt.'

Het gebruik van CIMS doorloopt volgens de DPIA CIMS release 1.0 de volgende fasen:

i. Het inladen van gegevens cliëntbeheer
ii. Het selecteren en oproepen van burgers uit een doelgroep
iii. De registratie van de vaccinatiegegevens
iv. Het oproepen voor de tweede en/of derde vaccinatie
v. Het evalueren van de binnen CIMS geregistreerde vaccinaties
vi. Het ophalen van gegevens voor de opvolgend zorgverlener
vii. De epidemiologische evaluatie ten behoeve van de vaccinatiegraad, effectiviteit, impact en veiligheid van de vaccinatie.

Onderstaand advies betreft de gegevensverwerking ten aanzien van het selecteren en oproepen van burgers uit een doelgroep (fase ii).

Ten aanzien van de DPIA zijn de volgende opmerkingen te plaatsen.

1. Inleiding – 1

Blijkbaar is voor gebruikmaking van de functionaliteit van CIMS 2.0 eerst in handmatige vorm uitvoering gegeven aan de gegevensverwerking selecteren en oproepen van doelgroepen. Hierbij wordt aangegeven dat er een informatiebeveiligings- en privacy risicoanalyse is uitgevoerd. Het is niet duidelijk in hoeverre de uitkomsten van deze uitgevoerde informatiebeveiligings- en privacy risicoanalyse onderdeel vormen van de beschrijving en beoordeling van de risico's van de voorgenomen verwerking in deze DPIA.

2. Voorstel – 2.1

Aangegeven wordt dat vanaf 26 februari het selecteren en oproepen geautomatiseerd zal worden uitgevoerd. Daar waar blijkbaar nu per opdracht een handmatige query gegenereerd wordt om gegevens uit CIMS te halen. In de DPIA komt niet naar voren wat precies verstaan wordt onder geautomatiseerd en welk gedeelte in het proces dit betreft. Om als organisatie zicht op de privacy risico's te verkrijgen is helderheid hierop van belang.

Na het aanmaken van de selectie worden NAW-gegevens van de geselecteerde personen verzameld. De DPIA en de procesplaat[4] maakt niet duidelijk op welke wijze het verzamelen van de geselecteerde personen plaatsvindt. Vindt hier een koppeling met een ander systeem plaats (BRP)? Helderheid hierop is van belang om als organisatie zicht op de privacy risico's van de betrokkenen te verkrijgen.

Aangegeven wordt dat het gecombineerde bestand vervolgens via gzip ingepakt wordt en in de database van CIMS wordt geplaatst. Het is onduidelijk hoe dit zich verhoudt tot het figuur uitnodiging proces (hoofdstuk 2.8) waar gesproken wordt over een tijdelijke opslag op de beheer server. Wat wordt bedoeld met de beheer server? Is dit bijvoorbeeld een dedicated beheer server van CIMS? Helderheid hierop is van belang om als organisatie zicht op de privacy risico's van de betrokkenen te verkrijgen.

Aangegeven staat dat de gedownloade bestand via filsender naar (momenteel) Xerox en later rechtstreekst naar de drukker zal plaatvinden. Een risico dat niet genoemd wordt is welke mogelijke risico's het verstrekken van de bestanden aan Xerox met zich meebrengt wetende dat Xerox een wereldwijd opererend Amerikaans bedrijf is. Daarnaast is het onduidelijk in hoeverre dit zich verhoudt tot de latere tekst dat de printbestanden rechtsreeks naar de drukker gaan. Het is hiermee onduidelijk

[4] Procesplaat oproepen 20210215

wat precies de rol van Xerox in het geheel is. Wetende dat in het overzicht van betrokken partijen Xerox als verwerker aangemerkt staat.

Voor transport van de printbestanden wordt gebruik gemaakt van filesender. Zowel de DPIA als de procesplaat geven geen nadere toelichting over filesender. Betreft dit een on-premise tool of wordt hier gebruik gemaakt van een dienst van een andere partij? Deze onvolledigheid leidt tot onvoldoende inzicht in de betrokken partijen en diens rol wat betreft verwerkingsverantwoordelijke, verwerker. Hiermee is het mede onduidelijk of met betreffende partijen verwerkersovereenkomsten noodzakelijk zijn.

3. Bewaartermijnen – 2.10

Blijkbaar vindt er een tijdelijke opslag van het printbestand op de beheer server plaats. Het advies is om in de DPIA aan te geven wat de bewaartermijn van deze opslag is.

4. Rechtsgrond – 3.1

Verwezen wordt naar de DPIA CIMS release 1.0. Let wel in paragraaf 3.1.3 wordt verwezen naar artikel 6, eerste een tweede lid Wpg. De FG verondersteld dat hier artikel 6**b** eerste en tweede lid Wpg mee bedoeld wordt.

5. Doelbinding – 3.4

In de DPIA wordt verwezen naar DPIA CIMS release 1.0. Echter hierin staat in paragraaf 2.4.8 weergegeven: 'Na het oproepen van personen, worden – voor zover de (zorgverleners van de) GGD-en de betrokkenen gaan vaccineren – aan de GGD-en een lijst met personen die door het RIVM zijn opgeroepen verstrekt.'

Het beginsel van doelbinding (artikel 5, eerste lid, onder b, van de AVG) brengt met zich mee dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en vervolgens niet verder op een met die doeleinden onverenigbare wijze mogen worden verwerkt. Gelet op het beginsel van doelbinding zal moeten worden nagegaan of de verwerking van de persoonsgegevens, te weten het verstrekken van een lijst opgeroepen personen verenigbaar is met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld. Hierbij dient onder meer rekening gehouden te worden met artikel 6, vierde lid, van de AVG. Daarnaast is het delen en verder verwerken van informatie tussen verschillende instanties alleen toegestaan met inachtneming van de beginselen van noodzakelijkheid en dataminimalisatie.

Het advies is om de doelbinding, de noodzakelijkheid en dataminimalisatie van de verstrekking van de lijst aan de GGD-en nader af te wegen, te duiden en de DPIA hierop aan te passen.

6. Rechten van de betrokkene – 3.6

Verwezen wordt naar de DPIA CIMS release 1.0, echter het is onduidelijk hoe invulling aan de rechten van de betrokkene wat betreft het oproepen en selecteren gegeven wordt. In de DPIA waarnaar verwezen wordt niet ingegaan op het recht op informatie ten aanzien zien van deze verwerking.

Het advies is om in de DPIA de rechten van de betrokkene duidelijker te omschrijven.

7. Risico's voor de rechten van de betrokkene – 3.8

Risico's die niet worden benoemd, maar wel aandacht behoeven zijn:

- De mogelijkheid dat de gebruiker via een scherm CIMS meerdere gegevens zou kunnen genereren die mogelijk in de oproepbrieven terecht zou kunnen komen, denk aan het per abuis opnemen van het BSN in de brief. Het advies om uit te leggen in hoeverre (en in welke maatregelen worden voorzien) dat een dergelijk risico niet kan voorkomen.

- Het risico dat met de verwerker geen verwerkersovereenkomst (overtreding art. 28 lid 3 AVG) is afgesloten. Dit kan leiden tot een boete van de toezichthouder en/of reputatieschade voor VWS. Hieraan gelinkt is het risico dat de verwerker niet voldoet aan de door VWS gestelde eisen als het voldoen aan de BIO[5].

Het advies is om in de DPIA deze risico's nader af te wegen, te duiden en de DPIA hierop aan te passen.

[5] Baseline Informatiebeveiliging Overheid