Departementaal VERTROUWELIJK.

Bijlage	**Advies 5.1.2e VWS DPIA Referentie DPIA GGD Contact**
Directie/concernonderdeel	IDirectie/ 5.1.2e - RDO
Naam 5.1.2e	5.1.2e
Contactgegevens:	5.1.2e @minvws.nl
Datum advies:	12 juli 2021

Inleiding 5.1.2e

De 5.1.2e van het ministerie VWS is op grond van het bepaalde in 5.1.2e 5.1.2e 5.1.2e Onderstaand advies heeft betrekking op de DPIA-versie 10 juni 2021.

Naast het geraadpleegde advies van 5.1.2e van de afzonderlijke GGD-en is tevens 5.1.2e van VWS om advies geraadpleegd om redenen dat[1]:
- VWS bij de ontwikkeling van de GGD Contact stelselverantwoordelijk is voor de inrichting en ontwikkeling van GGD-contact, en het informeren van de gebruikers voor de werking van de GGD-contact app. En daarbij ook verantwoordelijk is voor de (tijdelijk) hosting van GGD Contact;
- blijkt dat de minister van VWS, naast de GGD'en, tijdens de realisatiefase eindverantwoordelijk is voor bepaalde belangrijke deelelementen die bepalend zijn voor het functioneren van de GGD Contact App en de aansluiting van het BCO Portaal daarop. En om die reden de GGD'en en de minister van VWS moeten worden aangemerkt als gezamenlijk verwerkingsverantwoordelijk voor zover tijdens de ontwikkeling van de GGD Contact App sprake is van de verwerking van (bijzondere) persoonsgegevens.
- voor de minister van VWS geldt dat hij tijdens de praktijkfase aan te merken is als verwerker. Dit omdat hij tijdens de praktijkfase enkel zorgdraagt voor de (tijdelijke) hosting van de GGD Contact in opdracht van de GGD'en en geen zeggenschap heeft over het doel en de middelen van gegevensverwerking.

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 (U)AVG voldoen. Het uitvoeren van een data privacy impact assessment (DPIA) voor gegevensverwerkingen met een hoog privacyrisico 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 privacyrisico'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

[1] Zie referentie DPIA GGD contact pagina 21

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.

Bronbestanden

- Referentie DPIA GGD Contact, 10 juni 2021 inclusief bijlagen 4

Advies

Zoals in de DPIA aangegeven betreft het *'Het reguliere proces van BCO is lastig uitvoerbaar bij een pandemie zoals bij COVID-19 het geval is. Ter ondersteuning van het BCO Proces COVID-19 gaan GGD'en in Nederland gebruikmaken van een BCO-ondersteunende applicatie met het bijbehorende webportaal: GGD Contact.'* De DPIA dient als referentie-document voor iedere GGD afzonderlijk. Iedere GGD kan dit document gebruiken om deze om te zetten en aan te passen op haar eigen interne processen.

De DPIA is een goed leesbaar stuk met een duidelijke omschrijving van de verwerking. De 5.1.2e heeft de volgende opmerkingen bij de DPIA en adviseert daarmee rekening te houden. En de DPIA hierop aan te scherpen.

1. Inleiding –pg. 13

1.1 Waarschijnlijk is er een typo ingeslopen wat betreft de verantwoordelijkheid ten aan zien van Incident Management. Aangegeven staat: 'Incident Management (met inbegrip van monitoring) is verantwoordelijkheid GGD GHOR. VWS'. Betreft dit een gezamenlijke verantwoordelijkheid of is het incidentmanagement een volledige verantwoordelijkheid van GGD GHOR?

2. Gegevensverwerkingen –A2, pg. 18

2.1 Wanneer de index de eerste ziektedag niet wil invullen kan je de GGD Contact App niet gebruiken. Het is de vraag op welk moment dit keuzemoment plaatsvindt. Komt dit keuzemoment voor of nadat de index gegevens in de GGD-contact heeft ingevuld? Wat gebeurt er met de gegevens indien de betrokkenen niet eerste ziektedag wil invullen met de al ingevulde data?

3. Betrokken partijen en rolverdeling – A3, pg. 20

3.1 Aangegeven staat: *'Voor zover persoonsgegevens worden verwerkt bij de ontwikkeling van de GGD Contact App en het BCO Portaal heeft de minister daarvoor een verwerkingsgrondslag op basis van de vervulling van zijn taak van algemeen belang (artikel 6, eerste lid, aanhef en onder e, AVG jo. artikel 3, eerste lid jo. artikel 7, eerste lid Wpg). De verwachting is dat na het opleveren van de GGD Contact App de verwerking van persoonsgegevens niet meer noodzakelijk is voor het realiseren van de GGD Contact App en het BCO Portaal.'* Het is onduidelijk wat met voorgaande bedoeld wordt. Welke gegevens zijn dit en welke nut & noodzaak is er voor de verwerking van deze gegevens. Betekent dit dat bij de ontwikkeling van de GGG Contact App gewerkt is met zogeheten productiegegevens? Verduidelijk dit en geef aan welke mogelijke risico's dit met zich meebrengt (heeft gebracht) en hoe de mogelijke privacyrisico's beheerst zijn.

4. Noodzaak en evenredigheid – B13, pg. 44

4.1 Aangegeven staat: '*contactgegevens van de personen waarmee de index in contact is geweest en niet zijn gehele telefoonboek. Bij het geven van toestemming om het gehele adresboek weer te geven in de GGD Contact App worden dus ook contacten zichtbaar waarmee de index tijdens zijn besmettelijke periode niet in contact is geweest. Dit is dientengevolge een risico waar passende maatregelen op dienen te worden genomen. Door toepassing van privacy-by-design wordt hier rekening mee gehouden doordat enkel de namen uit het telefoonboek zichtbaar worden en overige informatie uit het adresboek achterwege blijft.*' Dus enkel de namen. Echter in de huidige versie krijgt betrokkene de tekst te zien: 'Wil je contactenlijst gebruiken om contactgegevens in te vullen? Alleen de contactgegevens die jij kiest worden gebruikt in de app. Bijvoorbeeld een achternaam of een telefoonnummer'. Dus niet alleen naam maar ook telefoonnummer. Dit is mede gelinieerd aan het risico nr. 3 pagina 52 'Verwerking van meer gegevens dan noodzakelijk'. Waarbij momenteel als standaardinstelling is opgenomen dat bij het verstrekken de gehele contactenlijst wordt ingeladen. In de DPIA is het advies opgenomen om als maatregel het advies van het privacy-team op te volgen om de mogelijkheid voor het ophalen van de gehele contactenlijst uit GGD Contact te verwijderen. En enkel het zelf selecteren van de contacten mogelijk te maken. De 5.1.2e van VWS onderschrijft dit advies en adviseert prioriteit aan de opvolging van deze maatregel te geven. Dit aangezien het meer verwerken van gegevens dan noodzakelijk in strijd is met artikel 5 AVG. Het verzamelen, verwerken, en delen van informatie is alleen toegestaan met inachtneming van de beginselen van noodzakelijkheid (artikel 8, tweede lid, van de EVRM) en dataminimalisatie (artikel 5, eerste lid, onder c, van de AVG). Deze beginselen eisen dat de hoeveelheid persoonsgegevens tot het noodzakelijke worden beperkt.

5. Risico's – C15, pg. 59

5.1 Als maatregel voor ongeautoriseerde inzage in het BCO Portaal is als maatregel het uitvoeren van een antecedentenonderzoek bij nieuwe medewerkers (ook bij samenwerkingspartners) opgenomen. Screening kan zeer ingrijpend zijn voor de privacy van de betrokkene waarbij persoonsgegevens verwerkt worden. Dat betekent dat de AVG en de UAVG van toepassing zijn. Een werkgever of inhuurder mag alleen screenen als hij daarbij aan bepaalde (wettelijke) voorwaarden voldoet. Een maatregel als het uitvoeren van een antecedentenonderzoek is onderdeel van reguliere bedrijfsvoeringsprocessen van de GGD-en. De noodzakelijkheid van het uitvoeren van dit onderzoek en de wijze waarop moet in een DPIA bij het reguliere BCO-proces bedrijfvoeringsproces worden onderbouwd. Het antecedentenonderzoek valt buiten het toezicht bereik van de 5.1.2e van VWS.

Bevindingen

De 5.1.2e adviseert de DPIA aan te scherpen op bovenstaande aanbevelingen en waar nodig het proces aan te passen.

Acties naar aanleiding van Advies 5.1.2e

Leg vast welke acties naar aanleiding van het advies van de 5.1.2e zijn uitgevoerd.

Bijlage 1

De belangrijkste regels voor de omgang met persoonsgegevens staan in de AVG vermeld. Naast de AVG draagt diverse andere Europese regelgeving bij aan de bescherming van persoonsgegevens, zoals:

- artikel 8 uit het *Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden* (EVRM);
  Op grond van dit artikel is geen inmenging van enig openbaar gezag toegestaan in de uitoefening van het recht op respect voor zijn privéleven, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen;
- artikel 8 van het *Handvest Grondrechten van de EU*;
  Dit artikel bepaalt onder meer dat persoonsgegevens eerlijk en voor bepaalde doeleinden moeten worden verwerkt, en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet;
- artikel 16 van het *Verdrag betreffende de werking van de Europese Unie* (VWEU);
  Dit artikel bepaalt dat eenieder in de Europese Unie recht heeft op bescherming van zijn persoonsgegevens;
- artikel 10, eerste lid, van de *Grondwet*;
  Dit artikel bepaalt dat eenieder recht heeft op eerbiediging van zijn persoonlijke levenssfeer, behoudens bij of krachtens de wet te stellen beperkingen.

Bijlage 2 Uitgangspunten bij de beoordeling van een GEB-PIA

Er zal uitgegaan worden van een zo laag mogelijke tot geen privacyrisico voor de rechten en vrijheden van betrokkenen op wie de gegevensverwerking betrekking heeft. D.w.z. de opzet en inrichting van de verwerking heeft een zo laag mogelijke tot geen impact op de persoonlijke levenssfeer van de betrokkenen. Dit gezien de gevoelige aard van de persoonsgegevens dan wel de hoeveelheid van persoonsgegevens en de mogelijke gevolgen die inzage door onbevoegden in de persoonsgegevens met zich meebrengen. Denk hierbij bijvoorbeeld aan:
Verlies van controle over hun persoonsgegevens of de onmogelijkheid hun rechten en vrijheden uit te oefenen;

- Discriminatie, stigmatisering en uitsluiting
- (blootstelling aan) identiteitsdiefstal of fraude
- Gezondheidsschade

Als wel bestuurlijke, politieke risico's die een onrechtmatige verwerking met zich meebrengen.

De belangrijkste uitgangspunten bij deze review zijn in hoeverre ...

- de scoping van de verwerking voldoende helder en onderbouwd is;
- het nut en de noodzaak van de (voorgenomen) verwerking voldoende aantoonbaar[2] aanwezig is;
- de gehele keten voldoende op privacy risico's bekeken is (denk ook aan uitbestede partijen, en onderaannemers);
- de verantwoordelijkheden en rollen van de verschillende stakeholders duidelijk en inzichtelijk beschreven zijn (*verwerkingsverantwoordelijke, (sub)verwerker, verstrekker* en *ontvanger)*;
- de persoonsgegevens verwerkt worden op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is (*„rechtmatigheid, behoorlijkheid* en *transparantie"*)[1];
- de persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt ("*doelbinding*")[1];
- de *proportionaliteit-* en *subsidiariteitsbeginselen* toegepast en aantoonbaar zijn;
- de persoonsgegevens toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (*„minimale gegevensverwerking"*)[1];
- de opzet en inrichting er voor zorgt dat de juistheid van de gegevens gewaarborgd is ("*juistheid*")[1];
- de persoonsgegevens worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is ("*opslagbeperking*")[1];
- de risico's van de gegevensverwerking (zowel voor gegevensuitwisseling, –opslag en het gebruik) voor de rechten en vrijheden van de betrokkenen inzichtelijk en aantoonbaar en onderbouwd zijn;
- door het nemen van passende technische of organisatorische maatregelen de persoonsgegevens op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging ("*integriteit en vertrouwelijkheid*")[1];
- de principes van *privacy-by-design* en *privacy-by-default* voldoende gehanteerd worden[3];
- een veilige en betrouwbare gegevensuitwisseling, -opslag en verwerking in lijn is met wet- en regelgeving en relevante standaarden zoals de Code voor Informatiebeveiliging (ISO 27001/2), ISO

[2] AVG, artikel 5
[3] AVG, artikel 25

7510, 7513 en de Baseline Informatiebeveiliging Overheid (BIO), specifieke bij de verwerking van toepassing zijnde wetgeving zoals WGBO;

- opslagbeperking ten aanzien van *bewaartermijnen* dan wel dataminimalisatie aantoonbaar toegepast is;
- het need-to-know principe toegepast is.

Let wel, voorgaande uitgangspunten zijn slechts enkele uitgangspunten voor het beoordelen van de DPIA en dient niet als een afvinklijst gehanteerd te worden maar geeft een illustratie waaraan een kwalitatief goed uitgevoerde DPIA moet voldoen. Naast voorgaande uitgangspunten wordt ook het proces van het tot stand komen van de DPIA beoordeeld. Aspecten die hierbij een rol spelen zijn onder andere: door wie is het proces begeleid, is er voldoende expertise betrokken bij de totstandkoming van de DPIA, op welk moment in het proces is de DPIA uitgevoerd?