Departementaal VERTROUWELIJK.

Bijlage **Advies Functionaris voor gegevensbescherming VWS DPIA CoronaCheck / CoronaCheck scanner app**

Contactgegevens: 5.1.2e @minvws.nl

Datum advies: 24 maart 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 verwerkingen in het kader van testbewijs voor de Fieldlabs situatie ('MVP pilots'). Dit advies heeft betrekking op de DPIA CoronaCheck / CoronaCheck scanner app, versie 23.03.2021. In een eerder stadium van de opzet van CoronaCheck / CornaCheck scanner app ten behoeve van fieldlabs evenementen is door de FG een advies[1] op de voorgenomen verwerking gegeven. Eerder uitgebrachte adviezen van de FG ten aanzien van CoronaCheck / CoronaCheck scanner app blijven van kracht.

Het betreft hier de Coronacheck / Coronacheck scanner app (hierna Coronacheck) welke ingezet wordt op de toepassing van het testbewijs bij het Fieldlabs evenement van 27 maart 2021.

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 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 staat aangegeven: '*Nederland wordt, net als de rest van de wereld, geconfronteerd met de uitbraak van het SARS-CoV-2, een virus dat kan leiden tot de ziekte COVID-19.De verspreiding van SARS-CoV-2 wordt beteugeld door diverse maatregelen. Daar waar veel mogelijkheden worden beperkt door een lockdown, ontstaat ook de behoefte om op een gecontroleerde manier de samenleving weer te openen.*

Het testbewijs is een bewijs dat iemand negatief is getest en dat tijdelijk geldig is. Dit bewijs kan worden gebruikt om toegang te geven tot specifieke evenementen en locaties. Het testbewijs maakt het (in combinatie met andere risicobeperkende maatregelen) mogelijk om daar waar verlichting van de lockdown mogelijk is, dit ook te doen.

Dit testbewijs en de applicaties CoronaCheck en CoronaCheck Scanner worden onder verantwoordelijkheid van de Minister van VWS ontwikkeld. Dit document bevat een Privacy Impact Assessment, (hierna: PIA) van het gebruik van persoonsgegevens[2] voor het testbewijs en de applicaties, conform artikel 35 van de Algemene Verordening Gegevensbescherming (hierna: AVG)'

[1] Advies Functionaris voor gegevensbescherming VWS DPIA CoronaCheck/CoronaCheck scanner app, d.d. 2 maart 2021

[2] Uitgangspunt van deze PIA is het voorgenomen gebruik van (persoons)gegevens zoals bekend op 21 februari 2021.

Binnen de scope van de DPIA valt:
- het ophalen van een (negatief) testresultaat bij een teststation;
- het generen van een testbewijs (in CoronaCheck);
- de validatie van het testresultaat bij een toegangsdeur (door CoronaCheck Scanner).

Buiten scope van de DPIA en daarmee buiten scope van het advies van de FG valt de gegevensverwerking ten behoeve van het testen, het verstrekken en de daarmee aan de orde zijn verwerkingen van persoonsgegevens door het teststation (welke binnen deze PIA als SON aangeduid). Wel worden er ter lering enkele separate opmerkingen door de FG VWS geplaatst.

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

1. Voorstel– A1

1.1 'Buiten scope DPIA':
- Is binnen de gegevensverwekingen van de teststations en SON duidelijk hoe de rollen zich verhouden?
- Email met PDF; wat wordt hier precies bedoelt?

1.2 Aangegeven staat op pagina 8: 'Zodra het testresultaat beschikbaar is, vult de persoon via de smartphone op een website van SON een token in (een unieke code).' Wiens website betreft dit? Is dit een website van de teststations of van SON. En indien het een website van SON betreft op basis van welke grondslag verwerkt SON deze gegevens. Daarnaast is het onduidelijk wie verwerkingsverantwoordelijke voor deze gegevensverwerking is. Verduidelijk dit.

1.3 De tekst: 'Zodra het testresultaat beschikbaar is, vult de persoon via de smartphone op een website van SON een token in (een unieke code). De persoon krijgt ter controle een SMS op de smartphone om het ophalen te bevestigen. Vervolgens wordt het testresultaat van de persoon vanuit de browser op de smartphone in de CoronaCheck app werden geladen.' Het is onduidelijk wat precies verstaan wordt onder de persoon krijgt ter controle een SMS op de smartphone om het ophalen te bevestigen. Betreft deze SMS een unieke code die in de app ingegeven moet worden? En hoe verhoudt dit zich dan tot de tekst welke in de demo app welke in de Apple store (d.d. 24.03.2021) te raadplegen is onder 'hoe werkt de CoronaCheck-app? Vul in de CoronaCheck-app jouw code in. Deze code krijg je in een email-bij je testresultaat.' Verduidelijk het proces.

1.4 Aangegeven staat op pagina 9: 'SON tekent het testresultaat cryptografisch, waarmee CoronaCheck kan controleren dat het testresultaat ook daadwerkelijk van SON afkomstig is. Het is onduidelijk of dit proces binnen of buiten de scope van de DPIA valt en onder wiens verwerkingsverantwoordelijkheid dit valt. Indien zo ja binnen de scope DPIA; maak duidelijk welke gegevensuitwisseling hierbij plaats vindt.

1.5 Ten aanzien van de fysieke variant, zie pagina 9: Het is onduidelijk met welk doel eerste letter voornaam, eerste letter achternaam geboortedag, - geboortemaand in het testresultaat opgenomen staan. Blijkbaar gaan deze attributen ook naar de Signing Service. Met welk doel vindt dit plaats? Dit in het licht dat bij het versturen van testbewijs aan de betrokkene (email met PDF) dergelijke gegeven niet meer aan de orde blijken te zijn. Later, in hoofdstuk 2 wordt wel gesteld dat: Deze attributen helpen de persoon om voor zichzelf vast te stellen of het testresultaat ook van henzelf is. Ontvangt de betrokkene dan eerst een fysiek testresultaat (hoe en in welke vorm?) dat hij/zij dan omzet test bewijs (hoe?). Verduidelijk dit proces en geef een onderbouwing met betrekking tot het doel voor het gebruik van de attributen (eerste letter voornaam, eerste letter achternaam geboortedag, - geboortemaand) aan.

2. Verwerkingen van persoonsgegevens – A2

2.1 In dit hoofdstuk staat aangegeven welke gegevens worden gebruikt. Hierbij wordt niet aangegeven onder welke categorie van persoonsgegevens deze vallen. Kan ervan uitgegaan worden dat gezien de context al deze opgesomde gegevens onder de categorie bijzondere persoonsgegevens vallen? Maak in de DPIA duidelijk in hoeverre:

- de informatie die door middel van de QR-code wordt getoond als (bijzonder) persoonsgegevens beschouwd dient te worden;
- het tot stand komen van de QR-code met als terugkoppeling wel/geen toegang aan te merken als een verwerking van persoonsgegevens
- de handeling van het uitlezen van de QR-code door de controleur met als terugkoppeling wel/geen toegang aan te merken als een verwerking van persoonsgegevens.
Verduidelijk dit.

2.2 Aangegeven staat op pagina 11: 'In het papieren testbewijs wordt een indicatie toegevoegd dat de QR code een papieren testbewijs is.' Het is onduidelijk wat verstaan wordt onder een indicatie toegevoegd. Verduidelijk dit.

2.3 Aangegeven staat dat in het testbewijs geboortedatum en geboortemaand van getest persoon, aangevuld met de eerste letter van de voornaam en de eerste letter van de achternaam opgenomen staat, terwijl in het schema op pagina 8 het testbewijs deze gegevens niet in zich heeft[3]. Verduidelijk dit.

3. Betrokken partijen

3.1 Het is onduidelijk welke rol Stichting Open NL heeft en hoe dit zich verhoudt tot de teststations. In hoeverre heeft Stichting Open NL wel/niet inzage en kan zich toegang tot de gegevens verschaffen. In principe is aangegeven dat de verstrekking van testresultaten buiten de scope van DPIA valt. Echter om een compleet beeld van de keten te hebben dient de rol van Stichting Open NL helder te zijn. Verduidelijk dit.

4. Ontvangers –A4

4.1 Aangegeven staat dat VWS de testbewijzen tekent door een signing service, maar geen inzicht heeft in de inhoud van de testresultaten of testbewijzen. Verduidelijk in hoeverre het risico aan de orde is dat de signing service als wel de leverancier van de configuratieserver inzage in de testresultaten of –bewijzen kunnen hebben en welke waarborgen er zijn om dit risico te verkleinen dan wel weg te nemen.

5. Juridisch en beleidsmatig kader – A10

5.1 Aangegeven staat dat het gebruik van Corona Check bedoeld is als een gebruik van gegevens, enkel ter uitoefening van een zuiver persoonlijke of huishoudelijke activiteit. De FG kan zich hier niet in vinden aangezien:
- een ip-adres verwerkt wordt ten behoeve van het proces;
- de informatie die doormiddel van de QR-code wordt getoond als een bijzonder persoonsgegevens beschouwd dient te worden;
- de context waarin de app ingezet wordt niet als zuiver persoonlijke of huishoudelijk activiteit beschouwd kan worden. De inzet van zowel de digitale als fysieke testbewijs is de inzet voor het wel / niet toegang verkrijgen tot een evenement. Waarmee bepaald wordt of men wel/niet ergens aan kan deelnemen. Dit beperkt zich niet tot alleen een privédomein aangelegenheid. Er is enkel sprake van huiselijk of huishoudelijk gebruik als persoonsgegeven worden verwerkt in een gezinssituatie. Dat is hier niet het geval. Maak duidelijk welke juridisch en beleidsmatig kader aan de orde is.

6. Bewaartermijnen – A11

6.1 Aangegeven staat op pagina 14: Het IP adres dat in de communicatie van en naar Configuratie Server en de Signing Service wordt gebruikt, wordt door de beheerder 7 dagen bewaard om bij incidenten deze te kunnen onderzoeken. Na deze 7 dagen worden deze automatisch verwijderd'. Ook staat aangegeven dat door de derde partij (Prolocation) de externe IP-adressen tijdelijk worden vervangen door een intern IP-adres. Betekent dit dat bij de Signing Service geen IP-adressen bewaard worden? Verduidelijk dit.

7. Rechtsgrond/ gebruik van bijzondere persoonsgegevens

[3] Mondeling is door de CPO aan de FG aangegeven dat deze gegevens zich niet in het testbewijs bevinden.

7.1 Aangegeven staat op pagina 15: 'De AVG is niet van toepassing wanneer persoonsgegevens worden verwerkt in het kader van een zuiver persoonlijke of huishoudelijke activiteit (op grond van artikel 2 lid 2 sub c AVG).' De FG is van mening dat hier geen sprake is van zuiver persoonlijke of huishoudelijke activiteit. Zie eerdere opmerking ten aanzien van persoonlijke of huishoudelijke activiteit bij punt 5.1 hierboven. Dit betekent dat een grondslag voor de verwerking van de persoonsgegevens aanwezig dient te zijn.

Nabrander ten tijde van het schrijven van het FG-advies: Als alternatief is aan de FG voorgelegd om toestemming als grondslag voor de verwerking van (bijzondere)persoonsgegevens in te bouwen in de Coronacheck app. Let op, denk ook na over de grondslag van toestemming ten aanzien van de fysieke testbewijs in te regelen.
Pas de DPIA hierop aan.

7.2 Maak duidelijk wat de noodzakelijke doorbrekingsgrond is, waarmee het verwerkingsverbod van artikel 9, eerste lid, AVG wordt doorbroken. Gezien de eerder gemelde nabrander ten schrijven van het FG-advies vormt artikel 9, tweede lid, onderdeel a, AVG (uitdrukkelijke toestemming) een bruikbare doorbrekingsgrond van het verwerkingsverbod uit artikel 9, eerste lid, AVG. Verduidelijk dit.

8. Beschrijving en beoordeling risico's voor de betrokkenen– C

8.1 De risico's voor de betrokkenen zijn beschreven vanuit het perspectief van het digitale testresultaten/-bewijs met gebruik van de CoronaCheck. De beschreven risico's en voorgenomen maatregelen zomen niet in op de mogelijke privacy risico's ten aanzien van het fysieke testresultaat/testbewijs proces. Pas dit aan.

Bevindingen FG

Wat betreft de grondslag adviseert de FG om en specifieke en heldere grondslag te gebruiken voor de inzet van CoronaCheck app ten behoeve van Field labs evenementen. Uit de nabrander ten tijde van het schrijven van het FG-advies is als alternatief aangegeven als grondslag voor de verwerking en de doorbreking van het verwerkingsverbod uitdrukkelijke toestemming te hanteren.

Door de toepassing van *security by design* en *privacy by design* (versleuteling, dataminimalisatie, het niet inladen van de direct herleidbare persoonsgegevens) is alles overziend, aannemelijk dat de verwerking geen hoog risico zal opleveren. En is de indruk dat met een goede implementatie en toepassing van de voorgestelde maatregel en waarborgen de geschetste privacy risico ten aanzien van het construct van de CoronaCheck app en CoronaCheck scanner beheersbaar zijn. De FG adviseert om de mogelijke privacy risico's ten aanzien van de fysieke testresultaten/testbewijzen duidelijker inzichtelijk te maken.

De FG adviseert de DPIA voor de helderheid en transparantie aan te scherpen op bovenstaande opmerkingen.