AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 (10)(2e) F 070 (10)(2e)
autoriteitpersoonsgegevens.nl

(10)(2g)

Vertrouwelijk/Aangetekend
De Minister van Volksgezondheid, Welzijn en Sport
T.a.v. de heer (10)(2e)
Postbus 20350
2500 EJ Den Haag

Datum
16 juli 2020

Ons kenmerk
(10)(2g)

Contactpersoon
(10)(2e)

Onderwerp
Verzoek om voorafgaande raadpleging - aanvullende informatie nodig

Geachte heer (10)(2e)

Naar aanleiding van uw verzoek om een voorafgaande raadpleging en de daarbij meegestuurde DPIA heeft de Autoriteit Persoonsgegevens (AP) een aantal vragen. Deze vragen richten zich op drie hoofdcategorieën: verwerkingsverantwoordelijkheid voor de verwerking; de verwerking en risico's; en techniek en framework. Dit betreft een eerste set vragen, de AP sluit niet uit dat er in het vervolg van de behandeling van de voorafgaande raadpleging nog aanvullende vragen gesteld zullen worden om een advies te kunnen uitbrengen.

1. Verwerkingsverantwoordelijk voor de verwerking
   a. Er is nu gekozen voor verwerkingsverantwoordelijkheid op 'twee niveaus' waarbij verwerkingsverantwoordelijkheid wordt gesplitst in beheer en inrichting (met de Minister van Volksgezondheid, Welzijn en Sport als verwerkingsverantwoordelijke) en de uitoefening van de rechten van betrokkenen (waarvoor betrokkene zich moet richten tot de eigen regionale GGD). Dit roept vragen op. Kunt u toelichten waarom hiervoor is gekozen en niet bijvoorbeeld enkel de minister van VWS aan te wijzen als verwerkingsverantwoordelijke? Dit staat immers het aanwijzen van een contactpersoon voor het uitoefenen van de rechten van betrokkenen niet in de weg (artikel 29 AVG).
   b. Het verzoek om voorafgaande raadpleging is ingediend door het ministerie van Volksgezondheid, Welzijn en Sport, welke aanvankelijk als verwerkingsverantwoordelijke is aangeduid. Uit de DPIA blijkt dat de verwerkingsverantwoordelijkheid bij zowel het ministerie als de verschillende regionale GGD'en komt te liggen. Dit zou betekenen dat het voorliggende verzoek om voorafgaande raadpleging niet ontvankelijk is wanneer het niet door

alle verwerkingsverantwoordelijke partijen is opgesteld, ondertekend en ingediend. Hoe ziet u de verwerkingsverantwoordelijkheid in relatie tot het verzoek om voorafgaande raadpleging? Kunt u ons een overzicht geven van de verantwoordelijke organisaties inclusief contactgegevens, contactpersonen en FG's?

c. Waarom is de rol van de GGD'en als verwerkingsverantwoordelijken terwijl hun rol bij de app zeer beperkt t.a.v. de gegevensverwerking?
d. Begrijpen we u goed dat u artikelen 3 en 7 van de Wpg voldoende specifiek vindt om als grondslag voor de verwerking van persoonsgegevens voor een notificatieapp te dienen en dat een soortgelijke zin zoals is opgenomen in het voorgestelde Artikel 6d van de Wpg voor de GGD'en met betrekking tot de verwerking van bijzondere persoonsgegevens niet nodig is?

2. De verwerking en risico's

a. De in de DPIA opgenomen risico's lijken grotendeels gebaseerd te zijn op technische risico's in relatie tot de gebruikte infrastructuur. Hoewel deze infrastructuur verband houdt met de verwerkingen ziet de AP nog geen uitgebreide afweging van de risico's voor de rechten en vrijheden van natuurlijke personen bij de voorgenomen verwerking. Kunt u toelichten hoe de identificatie van risico's heeft plaatsgevonden en welke rol de risico's voor de rechten en vrijheden van natuurlijke personen daarbij spelen?
b. Binnen de risicoanalyse lijkt terminologie door elkaar te lopen. Het bruto risico is het product van kans en impact voordat mitigerende maatregelen worden getroffen. Het netto risico is het restrisico. Deze begrippen worden niet consequent gebruikt. Zo wordt in 'risico' 16 van de bijlage al een mitigerende maatregel benoemd bij het bepalen van de impact. Daarnaast worden er kwaliteitscontroles genoemd waarbij niet duidelijk is of deze reeds zijn uitgevoerd of ze slechts gepland zijn. Kunt u toelichten of de nu gemaakte inschatting definitief is of dat er een nog een herziening is voorzien? Kunt u ook toelichten bij de risico's en mitigerende maatregelen waar het risico zich bevindt (bijvoorbeeld VWS, GGD'en, het framework van Google en Apple) en wie de mitigerende maatregel neemt?
c. Bij de inschatting van de risico's, onderdeel impact, lijkt geen gewicht te zijn toegekend aan de gewenst brede adaptatie van de app en de mogelijkheid dat ongewenste verwerkingen de rechten en vrijheden van een groot aantal natuurlijke personen raakt. Daar speelt bijvoorbeeld mee de mogelijkheid dat een aanval eenvoudig kan worden opgeschaald. Kunt u toelichten hoe dit is meegewogen in de afweging?
d. Bij de inschatting van de risico's, onderdeel kans, lijkt de kans dat een gerichte aanval wordt uitgevoerd vaak relatief laag te worden ingeschat terwijl wordt beoogd de app binnen heel Nederland te gaan gebruiken. Dit laatste brengt met zich dat op veel fysieke plaatsen kan worden getracht aanvallen uit te voeren die, indien ze succesvol zijn, mogelijk leiden tot waardevolle informatie over bewegingspatronen van, en mogelijke ziekteverschijnselen bij mensen. Een bekend voorbeeld zijn winkelcentra met apparatuur om Bluetooth en WiFi signalen op te vangen. Dit soort informatie kan van invloed zijn op de kans dat er ergens een aanval wordt uitgevoerd. Kunt u toelichten hoe dit is meegewogen in de afweging?

e. Voor het gebruik van de app is het inschakelen van Bluetooth noodzakelijk. Bluetooth bevat echter enkele bekende kwetsbaarheden en daaraan gerelateerd aanvallen.[1] Dit risico is niet geadresseerd. Daarbij geldt dat dit risico groter is als het gaat om (verouderde) Androidtoestellen. Kunt u toelichten waarom dit risico niet is onderkent en er geen differentiatie is toegepast naar besturingssystemen van mobiele telefoons?
f. De DPIA noemt het GGD-portaal maar gaat verder niet in op de verwerkingen die daarin plaatsvinden. Wat is de relatie tussen (verwerkingen binnen) het GGD-portaal en de app? Welke additionele risico's ontstaan, bijvoorbeeld, door verdere verwerkingen van gegevens door het college van Burgemeester en Wethouders voor andere doelen dan infectieziektebestrijding, en hoe zijn deze geadresseerd?
g. In de DPIA komt het daadwerkelijke uitoefenen van de rechten van natuurlijke personen en de wijze van organisatie daarvan nauwelijks aan de orde. Aangezien in deze constructie vele organisaties verantwoordelijkheden dragen, kan het onduidelijk zijn bij wie deze rechten uitgeoefend kunnen worden en hoe dit georganiseerd is. Kunt u aangeven welke organisatorische maatregelen zijn getroffen om het uitoefenen van de rechten van natuurlijke personen te waarborgen? Zijn de FG's van de GGD'en ook betrokken geweest bij het opstellen van de DPIA, onderschrijven ze de resultaten, ook die van de FG van VWS?

3. Techniek en framework

a. De door VWS uitgevoerde verwerkingen in en rondom de app leunen volledig op het framework dat is ontwikkeld door Google en Apple. Daarbij geeft VWS aan dat Google en Apple geen verwerker zijn. VWS betoogt dit middels een verwijzing naar een FAQ aangaande het framework van Google en Apple. Kunt u aangeven welke nadere informatie buiten deze FAQ bestaat die het standpunt van VWS in deze onderbouwt? Kunt u deze informatie aan de AP verschaffen?
b. Pagina 17 van de DPIA lijkt een aantal tegenstrijdigheden te bevatten hetgeen de transparantie niet ten goed komt. Een cruciaal voorbeeld daarvan is: "*De implementatiesoftware van het DP3T protocol (de app van VWS) verwerkt de TEKs, DKs en RPIs/contactcodes, én kan een risicoscore bepalen aan de hand van een in de app opgenomen set parameters en weegfactoren.*" Volgens de door Google en Apple geleverde documentatie (en zoals ook te zien is in de broncode van de VWS app) is de app zelf enkel verantwoordelijk voor het opvragen en uploaden van de TEKs en de download van de DKs. Alle andere verwerkingen worden in het framework van Google en Apple gedaan, afgeschermd van de app. Kunt u dit toelichten?
c. De ontwikkelaars van DP-3T stellen: "*We also strongly believe that Apple and Google should adopt our subsequent enhancements, detailed in our white paper, that increase user privacy. We also strongly encourage both companies to allow an external audit of their code to ensure its functionality corresponds to its specification.*"[2] Kunt u toelichten in hoeverre de aanbevelingen van DP-3T door VWS worden onderschreven en deze in het framework van Google en Apple zijn opgenomen?
d. Zijn de genoemde rapportages aangaande pentesten, code reviews, code quality en code test coverage voorhanden? Is deze informatie voorhanden met betrekking tot zowel het

[1] https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-veilig-gebruik-van-smartphones-en-tablets (14 juli 2020)
[2] https://github.com/DP-3T/documents#apple--google-exposure-notification (14 juli 2020)

AUTORITEIT
PERSOONSGEGEVENS

Datum
16 juli 2020

Ons kenmerk
(10)(2g)

framework van Google en Apple , de app, en de backend? Kunt u deze rapportages de AP verschaffen?

e. Kunt u aangeven welke juridische entiteit, met vestigingsgegevens, er verantwoordelijk is voor wat genoemd wordt het framework van Google en Apple ? Indien er sprake is van meerdere entiteiten, wat is dan de verhouding tussen deze entiteiten en wie is primair verantwoordelijk?

Reageer op tijd

De AP verzoekt u binnen 1 week na dagtekening van deze brief, dus uiterlijk op **23 juli 2020**, uw reactie met de beantwoording van alle bovenstaande vragen toe te sturen. In dit geval wil de AP, vanwege het grote belang dat u hecht aan de invoering van de corona notificatie app, uw aanvraag zo snel mogelijk, maar uiteraard zeer zorgvuldig beoordelen. Vermeld bij beantwoording al het overige dat u voor de beoordeling van uw verwerking van belang acht. Indien u daar prijs op stelt bestaat uiteraard de mogelijkheid de door u aangeleverde antwoorden en bijbehorende documentatie in een gesprek toe te lichten.

U kunt pas starten met het verwerken van de persoonsgegevens als wij de procedure van een voorafgaande raadpleging hebben afgerond. De termijn voor behandeling van uw verzoek om voorafgaande raadpleging wordt opgeschort totdat de AP alle gevraagde informatie van u heeft ontvangen. Verstrekt u de gevraagde informatie niet (tijdig)? Dan moet de AP op basis van de beschikbare informatie beoordelen of de voorgenomen verwerking voldoet aan de vereisten van de AVG.

Juridisch kader

Voor dit dossier geldt artikel 36, eerste lid, van de Algemene Verordening Gegevensbescherming (AVG) als juridisch kader.

Tot slot

Ik vertrouw erop u met deze brief voldoende te hebben geïnformeerd. Heeft u vragen over de procedure? Dan kunt u hierover met mij contact opnemen.

Hoogachtend,

Autoriteit Persoonsgegevens,
Namens deze,

(10)(2e)

Senior Inspecteur Systeemtoezicht

AUTORITEIT
PERSOONSGEGEVENS

Postbus 93374, 2509 AJ Den Haag

PostNL
Port Betaald
Port Payé
Pays-Bas

VOLKSGEZONDHEID
WELZIJN EN SPORT
17 JULI 2020
SCANPLAZA