AUTORITEIT
PERSOONSGEGEVENS

De Minister van Volksgezondheid, Welzijn en Sport
De heer H.M. De Jonge
Postbus 20350
2500 EJ Den Haag

Datum
06 augustus 2020

Ons kenmerk
z2020-11824

Contactpersoon

Onderwerp
Advies op voorafgaande raadpleging COVID19 notificatie-app

Samenvatting
De Autoriteit Persoonsgegevens heeft op 7 juli 2020 een verzoek om voorafgaande raadpleging ontvangen van de Minister van Volksgezondheid, Welzijn en Sport betreffende het voornemen om persoonsgegevens te verwerken in de COVID19 notificatie-app. De AP constateert dat dit een samenstel van verwerkingen betreft, hoofdzakelijk de notificatie-app-software welke door het ministerie van Volksgezondheid, Welzijn en Sport is ontwikkeld, het Google Apple Exposure Notification framework waarop de notificatie-app-software is gebaseerd, en de backend server die uitwisseling van gegevens faciliteert. De AP merkt op dat de voorgenomen verwerking zal worden uitgevoerd onder gezamenlijke verwerkingsverantwoordelijkheid van de minister van Volksgezondheid, Welzijn en Sport, en de vijfentwintig regionale GGD'en.

De AP heeft op basis van de documentatie de voorgenomen verwerking beoordeeld en adviseert om niet te starten met de voorgenomen verwerking totdat de in het advies genoemde maatregelen zijn getroffen en adviezen in acht zijn genomen.

Om de verwerking rechtmatig uit te voeren binnen de kaders van de AVG geeft de AP aan dat de volgende maatregelen noodzakelijk zijn:

- Er moeten afspraken gemaakt worden met Google en Apple betreffende het Google Apple Exposure Notification framework;
- Zonder wettelijke grondslag is de inzet van de notificatie-app niet mogelijk;
- De backend server moet voldoen aan AVG-standaarden.

In dit advies vindt u nadere toelichting op bovenstaande maatregelen en worden verdere adviezen gegeven die u in acht dient te nemen om met de verwerking van start te kunnen gaan.

Inhoudsopgave

1. Inleiding

Op 7 juli 2020 heeft u – ingevolge artikel 36, eerste lid, van de Algemene Verordening Gegevensbescherming (AVG) – bij de Autoriteit Persoonsgegevens (AP) een verzoek om voorafgaande raadpleging ingediend (hierna: "het verzoek"). Het verzoek betreft een voorgenomen verwerking van persoonsgegevens betreffende de COVID-19 notificatie-app ("*CoronaMelder*") (hierna: notificatie-app).

Ingevolge artikel 58, eerste, tweede en derde lid van de AVG behandelt de AP het verzoek teneinde de verwerkingsverantwoordelijke(n) of de verwerker te waarschuwen indien met de voorgenomen verwerking(en) waarschijnlijk inbreuk op bepalingen van de AVG wordt gemaakt. Hierbij beoordeelt de AP de voorgelegde gegevensbeschermingseffectbeoordeling krachtens artikel 35 van de AVG met daarbij in het bijzonder de maatregelen die genomen zijn om het risico te beperken.

1.1 Verwerkingsverantwoordelijke organisaties voorgenomen verwerking

De verwerkingsverantwoordelijke organisaties inzake de voorgenomen verwerking zijn:

- De Minister van Volksgezondheid, Welzijn en Sport (hierna: "de Minister")
- GGD Amsterdam
- GGD Brabant –Zuidoost
- GGD Drenthe
- GGD Flevoland
- GGD Fryslân
- GGD Gelderland-Zuid
- GGD Gooi en Vechtstreek
- GGD Groningen
- GGD Haaglanden
- GGD Hart voor Brabant
- GGD Hollands Midden
- GGD Hollands Noorden
- GGD IJsselland
- GGD Kennemerland
- GGD Limburg-Noord
- GGD Noord- en Oost Gelderland
- GGD Regio Utrecht
- GGD Rotterdam Rijnmond
- GGD Twente
- GGD West Brabant
- GGD Zaanstreek-Waterland
- GGD Zeeland
- GGD Zuid-Holland Zuid (Dienst Gezondheid en Jeugd Zuid-Holland Zuid)
- GGD Zuid Limburg
- Veiligheids- en Gezondheidsregio Gelderland Midden

De AP merkt bovenstaande zesentwintig organisaties aan als gezamenlijke verwerkingsverantwoordelijken in de zin van artikel 26 AVG voor de voorgenomen verwerking. De Minister is contactpersoon voor het verzoek om voorafgaande raadpleging.

1.2 Achtergrond

Op 6 april 2020 adviseerde het Outbreak Management Team (OMT) de Minister om "zo snel mogelijk de mogelijkheden voor ondersteuning van bron- en contactopsporing m.b.v. mobiele applicaties te onderzoeken. Het OMT acht dit noodzakelijk voor de toekomstige fase in aanvulling op reguliere bron- en contactopsporing door de GGD'en. Het OMT heeft een voorkeur voor een populatiegebaseerde aanpak gebruikmakend van technieken die de privacy van eindgebruikers waarborgen conform de AVG-wetgeving"[1]. Naar aanleiding van dit advies startte de Minister een verkenning die leidde tot de zogenoemde openbare *appathon.* In het weekend van 18 en 19 april 2020 zijn een zevental digitale ondersteuningsoplossingen gepresenteerd. Experts vanuit diverse relevante expertises konden zich uitspreken om de apps te verbeteren. Het bleek dat de apps onvoldoende volwassen waren om te toetsen aan de gestelde randvoorwaarden en verwachtingen, waarna de Minister besloot zelf tot ontwikkeling van een app over te gaan.[2]

Op 9 juni 2020 bracht de AP advies uit over het wetsvoorstel Tijdelijke wet maatregelen COVID-19. Onderdeel van dit wetsvoorstel was een wettelijke verankering van de in ontwikkeling zijnde app.[3] De Minister besloot later de app uit het voornoemde wetsvoorstel te halen en onder te brengen in een apart wetsvoorstel Tijdelijke wet notificatieapplicatie. Deze wet is vooralsnog niet aanhangig gemaakt bij de Tweede Kamer.

2. Procedureverloop verzoek om voorafgaande raadpleging

- Op 7 juli 2020 verzochten de verwerkingsverantwoordelijken (bij name van de Minister van Volksgezondheid, Welzijn en Sport) de AP om een voorafgaande raadpleging. Hiervoor zond het ministerie de gegevensbeschermingseffectbeoordeling (*Data Protection Impact Assesment*, (DPIA)) op 8 juli na, met daarbij het advies van de Functionaris voor Gegevensbescherming (hierna: FG) van het ministerie van Volksgezondheid, Welzijn en Sport.
- Op 8 juli 2020 bevestigde de AP de ontvangst van het verzoek om voorafgaande raadpleging per brief aan de Minister. De behandeltermijn startte op 8 juli 2020.
- Op 16 juli 2020 verzocht de AP de Minister per brief om aanvullende informatie. Hiermee is de behandeltermijn opgeschort vanaf 16 juli 2020 tot het moment dat de aanvullende informatie volledig is aangeleverd. Diezelfde dag lichtte de AP deze vragen en de mogelijkheden van (eventueel in delen) aanleveren van informatie in een telefonisch gesprek toe aan de Minister.
- Op 23 juli 2020 leverde de Minister aanvullende informatie in één document aan de AP aan ter beantwoording van de gestelde vragen. De termijn, die was opgeschort per 16 juli 2020, is daarmee per 23 juli 2020 weer gaan lopen.
- Op 24 juli 2020 bevestigde de AP de ontvangst van deze informatie per brief aan de Minister.
- Op 6 augustus 2020 brengt de AP formeel advies uit aan de Minister en sluit daarmee de procedure van voorafgaande raadpleging af.

[1] Advies n.a.v. 63e OMT COVID19, d.d. 6 april 2020, 0034/2020 LCI/JvD/at/mm
[2] Zie nieuwsbericht "AP: privacy corona-apps niet aangetoond", 20 april 2020, https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-privacy-corona-apps-niet-aangetoond.
[3] Zie bijlage voor het advies van de AP op het wetsvoorstel Tijdelijke wet maatregelen COVID-19.

Ingevolge artikel 36, derde lid, van de AVG heeft u de volgende informatie verstrekt:

1. DPIA notificatie-app
2. Advies FG VWS DPIA notificatie-app
3. Reactie VWS op FG-advies
4. DPIA notificatie-app vaststelling met handtekening
5. Bijbehorende informatie[4]
6. Aanvullende informatie, door de Minister aangeleverd op 23 juli 2020

De Minister heeft in de DPIA 32 risico's geïdentificeerd, waarvan vier met een hoge impact en drie met een hoge kans. De Minister geeft aan dat met de te nemen maatregelen de verwerking geen hoog risico zal opleveren. Toch besloot de Minister, conform het advies van de FG en vanwege het maatschappelijke belang, de voorgenomen verwerking aan de AP voor te leggen in een verzoek om voorafgaande raadpleging. De aard van de verwerking rechtvaardigt volgens de AP een verzoek om voorafgaande raadpleging.

De Minister past diverse organisatorische en technische maatregelen toe om de risico's te mitigeren. Voor een overzicht verwijzen wij naar de DPIA, aangezien de Minister geen van de risico's als hoog indiceert.

Gelet op de verkregen informatie stelt de AP vast dat sprake is van een voorgenomen verwerking van persoonsgegevens waarop de AVG van toepassing is (artikel 2 en 3 van de AVG). De Minister geeft met het oog op maximale zorgvuldigheid aan dat er zekerheidshalve van is uitgegaan dat in alle fases van de verwerking persoonsgegevens worden verwerkt.[5] De AP heeft geen reden om hiervan af te wijken in dit advies.

3. Feitelijke weergave voorgenomen verwerking

De voorgenomen verwerking van persoonsgegevens vindt plaats met een notificatie-app die fysieke contactmomenten van een gebruiker met andere gebruikers van de notificatie-app vastlegt. De gebruiker krijgt een notificatie als bij één van deze contacten een COVID-19 infectie wordt geconstateerd en diegene dit meldt in de notificatie-app. Het betreft contactmomenten waarbij de gebruiker ten minste een vastgestelde tijdsperiode in de nabijheid is geweest van één of meer andere gebruikers, waardoor een verhoogde kans op besmetting met COVID-19 bestaat. De gebruiker krijgt via de app vervolgens het advies om contact op te nemen met de regionale GGD.

De notificatie-app maakt gebruik van het Google Apple Exposure Notification framework, zoals dat recent is geïntegreerd in de mobiele besturingssystemen van Google (Android) en Apple (iOS), en Bluetooth Low Energy protocol (BLE).[6] De gebruiker downloadt de notificatie-app (genaamd "*CoronaMelder*") in de Google Play Store of Apple App Store en installeert deze op zijn of haar smartphone.

[4] Bijbehorende informatie bestaat uit:
Wetsvoorstel notificatie app
Memorie van Toelichting notificatie app
[5] DPIA notificatie-app, pagina 13
[6] Zijnde: Google LLC (1600 Amphitheatre Parkway, Mountain View, California 94043, Verenigde Staten van Amerika) en Apple Inc. (1 Apple Park Way, Cupertino, California, Verenigde Staten van Amerika).

De notificatie-app zendt regelmatig wisselende codes uit (*Rolling Proximity Indicator*, RPI) die andere gebruikers van de app ontvangen die in de directe nabijheid zijn. Deze codes zijn afgeleid van een dagelijks gegenereerde blootstellingssleutel (*Temporary Exposure Key*, TEK). De nabijheid tussen twee telefoons wordt bepaald door de signaalsterkte van het bluetooth-signaal en de duur van de uitwisseling. De uitgewisselde codes van andere telefoons en de eigen blootstellingssleutels worden 14 dagen bewaard op de smartphone van de gebruiker.

Wanneer GGD constateert dat een gebruiker positief test op COVID-19 kan deze gebruiker ervoor kiezen om zijn blootstellingssleutels met een unieke autorisatiecode naar de backend server te sturen. Deze backend server zorgt voor onder andere de controle en uitwisseling van de codes tussen gebruikers en de GGD. De gebruiker genereert de autorisatiecode zelf, in de app. Ter validatie van deze code, vraagt de GGD de gebruiker om naar een bepaald scherm in de app te gaan en de code van zes tekens op te lezen. De GGD plaatst deze code, met de datum van de eerste ziektedag, in het GGD-portaal van de app. De backend server accepteert alleen blootstellingssleutels van gebruikers als een GGD-medewerker binnen 24 uur de autorisatiecode separaat bevestigt in het systeem. Dit dient moedwillige valse meldingen te voorkomen.

Met de bevestiging, door middel van de autorisatiecode worden op de blootstellingssleutels geconverteerd naar diagnosesleutels (waarmee de blootstelling en het risico worden berekend) die beschikbaar worden gemaakt op de server. Deze worden periodiek opgehaald door de smartphones van andere gebruikers waarop de app is geïnstalleerd.

Het Google Apple Exposure Notification framework berekent op de smartphone van de gebruikers voor elk van deze diagnosesleutels de bijbehorende afgeleide wisselende codes en controleert of er een match is met de op de smartphone opgeslagen uitgewisselde codes. Als er een match is krijgt de gebruiker een notificatie, inclusief dag waarop het contact heeft plaatsgevonden.

De voorgenomen verwerking vindt plaats onder verwerkingsverantwoordelijkheid van de Minister en de 25 Gemeentelijke Gezondheidsdiensten (GGD'en). Het Google Apple Exposure Notification framework waarop de app is gebouwd, is afkomstig en onder beheer van Google en Apple. De partij die de backend server zal leveren is ten tijde van dit advies nog niet bekend.

Aan bovenstaande feitelijke weergave van de voorgenomen verwerking wordt in dit advies als geheel gerefereerd als "de verwerking", ook als het onderdelen van de verwerking of samengestelde verwerkingen binnen het geheel betreft.

3.1 Over het advies

Dit advies is alleen geschreven voor de situatie zoals deze door de Minister is geschetst in het verzoek om voorafgaande raadpleging. Dit advies gaat dus over de situatie waarin een app van het ministerie van VWS interacteert met het Google Apple Exposure Notification framework en gekoppeld is aan processen bij GGD'en in Nederland. Ten aanzien van het Google Apple Exposure Notification framework, geldt dit advies dan ook niet voor het voornemen van Google en Apple om een tweede fase van het Google Apple Exposure Notification framework in te gaan (zie ook 4.3.2).

4. Beoordeling voorgenomen verwerking

De AP heeft zich een beeld gevormd van de rechtmatigheid van de door u beschreven voorgenomen gegevensverwerking tegen de achtergrond van de vereiste waarborgen uit de AVG. Voorts zijn met name de risicovolle aspecten van de voorgenomen verwerking beoordeeld.

Deze beoordeling is gebaseerd op de hiervoor onder 2 genoemde informatie die de Minister verstrekte in het kader van het verzoek en in het bijzonder de DPIA d.d. 8 juli 2020.

4.1 Vooraf

De AP merkt op dat de Minister heeft besloten een ethische toets uit te voeren in relatie tot het gebruik van de app en procedures daaromtrent. Bij zo'n potentieel ingrijpend middel wordt de wenselijkheid van de inzet daarvan dan ook mede bepaald door de beantwoording van ethische vraagstukken. Op deze wijze wordt niet alleen gekeken naar wat technisch kan en wat juridisch eventueel zou mogen maar ook naar de vraag of het middel past binnen de maatschappij waarin we leven. De AP moedigt de inzet van een ethische toets of assessment niet alleen voorafgaand, maar ook tijdens een verwerking aan. Het monitoren van de impact van het gebruik van de notificatie-app op individuen, groepen en de samenleving als geheel kan ook bijdragen aan het doorlopende proces van actualiseren, versterken en aanpassen van waarborgen voor de gegevensbescherming. Deze verwerking valt of staat bij het vertrouwen dat burgers stellen in de verwerking en de verantwoordelijke organisaties, ook hierbij stimuleert de AP de doorlopende inzet van een ethisch assessment als onderdeel van de kernwaarden transparantie en behoorlijkheid uit de AVG.

De AP constateert op basis van de ontvangen informatie dat de voorgenomen verwerking een samenstel van verwerkingen betreft:

- de notificatie-app software voor Android en iOS (genaamd CoronaMelder);
- de backend server waarvan de uitvoerende partij nog onbekend is, met:
    - een tijdelijke opslag voor de diagnosesleutels (TEK's)
    - een koppeling met het GGD-portaal ten behoeve van het invoeren van autorisatiecodes
    - een Application Programming Interface (API) voor het uitwisselen van gegevens tussen de mobiele applicatie en de backend
- het Google Apple Exposure Notification framework, dat de technische basis biedt voor uitwisseling van nabijheidsgegevens via Bluetooth Low Energy waarop de app en de backend server functioneren.

In de DPIA staat beschreven dat de Belastingdienst zorg draagt voor de backend server. Inmiddels heeft de Belastingdienst zich teruggetrokken en is er geen vervanger aangedragen. De AP kan zich geen oordeel vormen over dit onderdeel van de verwerking.

4.2 Overzicht Google Apple Exposure Notification framework

Een samenwerking tussen Google en Apple resulteerde in het Google Apple Exposure Notification framework. Deze samenwerking heeft de intentie om wereldwijd overheden en gezondheidsautoriteiten op een privacyvriendelijke manier te ondersteunen in het bron- en contactonderzoek ten aanzien van COVID-19. Het framework maakt, in de vorm van een API, functionaliteiten van de hardware en het besturingssysteem toegankelijk voor softwareontwikkelaars van de gezondheidsautoriteiten. Deze kunnen een app bouwen om gebruik te maken van deze functionaliteiten zoals ook het voornemen is voor de Nederlandse notificatie-app.

Google en Apple hebben bij de introductie van het framework aangekondigd dat hun oplossing uit twee fasen bestaat, namelijk de eerste fase waar de notificatie-app op aansluit en een tweede fase waarin het framework, volgens de plannen van Google en Apple, ook zelfstandig zou moeten gaan functioneren.[7] Deze beoordeling gaat kort op beide fasen in:

4.2.1 Eerste fase

De API's van Google en Apple zijn niet volledig open source ontwikkeld, waardoor de AP, naast de DPIA, haar advies heeft moeten baseren op de specificaties en het deel van de broncode dat Google en Apple eind juli openbaar maakten. Op basis daarvan constateert de AP dat de beschrijving in de DPIA niet overeenkomen met de werking zoals beschreven door Google en Apple. Zo geeft de notificatie-app de parameters voor risicobepaling en de opgehaalde blootstellingssleutel door aan het Google Apple Exposure Notification framework. Het framework berekent vervolgens de kans op een risicovol contact en geeft dit terug aan de notificatie-app, waarna de app een notificatie toont aan de gebruiker. De uitleg in de DPIA komt daarmee niet overeen met de uitleg van het Google Apple Exposure Notification framework, zoals gepubliceerd door Google en Apple.

De AP is voorts hetzelfde standpunt toegedaan als meerdere experts, zoals het team achter het Decentralized Privacy-Preserving Proximity Tracing-systeem (DP3T),[8] de auteurs van het "Mind the GAP" paper[9] en Trinity College Dublin,[10] namelijk dat er pas sprake is van een volledig open source-oplossing als ook het Google Apple Exposure Notification framework volledig open source is, en inzicht geboden wordt in de integratie met onderdelen van de mobiele besturingssystemen Android en iOS.

Uit de specificaties van het Google Apple Exposure Notification framework blijkt dat het in grote lijnen overeenkomt met DP3T. De AP onderschrijft dat het team achter het DP3T-systeem een hoog niveau van gegevensbescherming nastreeft. Dat Google en Apple en daarmee ook het ministerie van VWS dit systeem volgen is een begrijpelijke keuze. Wel wil de AP opmerken dat het team achter DP3T privacyverbeteringen heeft doorgevoerd aan het systeem die nog niet door Google en Apple in het Google Apple Exposure Notification framework zijn opgenomen. Specifiek doelt de AP dan op:

- De aanbeveling om een TEK maximaal 2-4 uur geldig te laten zijn in plaats van 24 uur (dit vermindert het risico op het volgen van gebruikers van de notificatie-app);
- De techniek 'EphID Spreading With Secret Sharing' waarbij de door middel van Bluetooth uitgezonden identifier wordt opgedeeld in stukken. Hierdoor wordt het lastiger voor een aanvaller die kort in de buurt is om de opgevangen Bluetooth-beacons te correleren aan een persoon, maar ook het opvangen van Bluetooth-beacons op afstand wordt lastiger.[11]

[7] Apple & Google, Exposure Notification – Frequently Asked Questions – mei 2020, v.1.1, p. 3, geraadpleegd op 03-08-2020.
[8] https://github.com/DP-3T/documents#apple--google-exposure-notification: "We also strongly encourage [Apple and Google] to allow an external audit of their code to ensure its functionality corresponds to its specification." Laatst bezocht op 30-07-2020.
[9] https://arxiv.org/pdf/2006.05914.pdf: "To increase trust in and public adoption of contact tracing apps, it is not only necessary to open source the national contact tracing app codes, but also the corresponding operating system functionality by Google and Apple. This is where the "magic" happens, and this is another part where potential privacy leaks could occur." Laatst bezocht op 30-07-2020.
[10] https://www.scss.tcd.ie/Doug.Leith/pubs/contact_tracing_app_traffic.pdf: "We note the health authority client app component of these contact tracing apps has generally received considerable public scrutiny and typically has a Data Protection Impact Assessment, whereas no such public documents exist for the GAEN component of these apps. Extending public governance to the full contact tracing ecosystem, not just of the health authority client app component, therefore seems to be urgently needed if public confidence is to be maintained.". Laatst bezocht op 30-07-2020.
[11] https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf, pagina 38 , geraadpleegd op 03-08-2020.

4.2.2 Tweede fase

Google en Apple hebben beschreven dat er plannen zijn voor een tweede fase die in de komende maanden beschikbaar zou moet komen. Of dit ook voor Nederland geldt hebben zij niet duidelijk gemaakt. De twee bedrijven zijn voornemens de tweede fase van het framework via een update van Android en iOS aan te bieden. Vanaf die update is er geen notificatie-app vanuit een gezondheidsautoriteit meer nodig voor de uitwisseling van blootstellingssleutels en hun afgeleiden. Ook voor het bepalen of er een match is, is geen notificatie-app nodig. Enkel na de notificatie van de gebruiker wordt gevraagd om de lokale of nationale notificatie-app te installeren en contact op te nemen met lokale autoriteiten. Dit impliceert dat Google en Apple op dit moment een volledige infrastructuur ontwikkelen om deze fase te kunnen faciliteren op basis van de documentatie die Google en Apple beschikbaar hebben gemaakt. Hoewel de beoordeling in het kader van de voorafgaande raadpleging geen betrekking heeft op de tweede fase, verzoekt de AP de Minister nadrukkelijk om de ontwikkelingen van deze tweede fase nauwgezet te volgen en de implicaties op de notificatie-app met betrekking tot de AVG en de publieke taak waarop deze notificatie-app is gestoeld doorlopend te beoordelen.

4.3 Beoordeling juridische onderbouwing

Elke verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn. De AP heeft getoetst of de in de DPIA opgenomen onderbouwing aannemelijk maakt dat deze beginselen voldoende in acht zijn genomen.

In het navolgende beoordeelt de AP allereerst of een rechtmatige grondslag voor de verwerking aanwezig is in combinatie met een uitzonderingsgrond voor de verwerking van bijzondere persoonsgegevens. Vervolgens beoordeelt de AP de noodzakelijkheid en effectiviteit van de notificatie-app. Tot slot maakt de AP enkele opmerkingen over toestemming als rechtsgrondslag en de vereiste toestemming in het kader van de Telecommunicatiewet.

De AP concludeert in het navolgende dat zonder (een verbeterd) wetsvoorstel Tijdelijke wet notificatieapplicatie er onvoldoende juridische grond is de verwerking te starten.

4.3.1 Grondslag voor verwerking

Bij de onderhavige voorgenomen verwerking van persoonsgegevens worden volgens de DPIA in meerdere fases bijzondere categorieën van persoonsgegevens verwerkt, namelijk persoonsgegevens betreffende de gezondheid van de betrokkene. Hieronder vallen bijvoorbeeld gegevens over (positief geteste) besmettingen met het COVID-19 virus, de categorie van (kans op) besmetting daarvan in de afgelopen dagen, de eerste dag van de ziekteverschijnselen en aanwijzingen voor een gelopen risico op besmetting met het COVID-19 virus. In beginsel is het verboden bijzondere categorieën van persoonsgegevens te verwerken, tenzij een beroep kan worden gedaan op een van de uitzonderingsgronden in artikel 9 AVG. Indien een beroep wordt gedaan op een uitzondering zoals voorzien in artikel 9, tweede lid, onder i, AVG (de verwerking om redenen van algemeen belang op het gebied van volksgezondheid), dan moet dat in wetgeving worden vastgelegd. Die wetgeving moet bij zo'n uitzondering voldoende specifiek zijn en voorzien in gepaste waarborgen om de rechten en vrijheden van betrokkenen te waarborgen.

Volgens de DPIA en de antwoorden die de Minister op 23 juli 2020 gaf op de vragen die de AP stelde is de verwerking van persoonsgegevens gebaseerd op de grondslag uit artikel 6, eerste lid, onder e, AVG: de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of een taak in het kader van de uitoefening van het openbaar gezag (hierna kortweg *publieke taak*). De publieke taak is volgens de

DPIA terug te voeren op artikel 3 en 7 Wet publieke gezondheid (Wpg) als het gaat om de Minister en op artikel 6, eerste lid, onder c, in combinatie met artikel 14 Wpg als het gaat om de GGD.

Verwijzend naar EDPB-guidelines 04/2020 merkt de AP op dat de rechtsgrondslag publieke taak in zijn algemeenheid de best passende grondslag voor onderhavige verwerking is.[12] Artikel 6, derde lid, AVG stelt eisen aan de wettelijke invulling van een dergelijke publieke taak. EDPB-guidelines 04/2020 stelt hierover dat dit inhoudt dat onder meer waarborgen zoals een duidelijke doelomschrijving en een beperking voor de verdere verwerking van gegevens in de wet moeten worden opgenomen, net als een duidelijke specificering van de verwerkingsverantwoordelijke(n). Het hanteren van de publieke taak van de Minister en de GGD als grondslag voor de notificatie-app wil niet zeggen dat het vrijwillige karakter van de verwerking wordt beperkt. Vanwege de wettelijke waarborgen kan de betrokkene zelf kiezen of hij of zij de app installeert en bij een eventuele besmetting kiezen of de benodigde codes in de app worden gedeeld zodat andere gebruikers een notificatie (kunnen) ontvangen.

Vanwege de gezamenlijke verwerkingsverantwoordelijkheid moeten alle partijen zelfstandig beschikken over een rechtmatige verwerkingsgrondslag. De AP constateert dat de Minister afwijkt van het advies van de AP op het wetsvoorstel Tijdelijke wet maatregelen COVID-19. Met name is de Minister van mening dat de huidige publieke taak van hemzelf voldoende is opgenomen in de Wpg. Uit de artikelen 3 en 7 Wpg en de toelichting daarop blijkt dat hierin is geregeld dat de Minister de bevoegdheid heeft om de leiding te geven aan de bestrijding van infectieziekten zoals COVID-19. In dat kader kan de Minister de voorzitter van de veiligheidsregio opdragen hoe de bestrijding ter hand te nemen (Artikel 7, eerste lid, van de Wpg). Daarnaast heeft de Minister de taak om de kwaliteit en doelmatigheid van de publieke gezondheidszorg te bevorderen en draagt de Minister tevens zorg voor de instandhouding en verbetering van de landelijke ondersteuningsstructuur (artikel 3, eerste lid, van de Wpg). Uit deze bepalingen kan worden afgeleid dat de Minister bevoegd is de burgemeesters aanwijzingen te geven over hoe zij gebruik moeten maken van hun eigen bevoegdheden, bijvoorbeeld die ze hebben uit hoofde van hoofdstuk V van de Wpg. De AP is van oordeel dat uit de bevoegdheid en taak om leiding te geven aan de bestrijding echter geen zelfstandige grondslag voor de verwerking van (bijzondere) persoonsgegevens kan worden afgeleid. Deze dient nader te worden geëxpliceerd. De voorgestelde invoering van artikel 6d Wpg in het wetsvoorstel Tijdelijke wet notificatieapplicatie biedt de mogelijkheid om deze toevoeging alsnog in te voeren en dit probleem op te lossen.

Het voorgaande schuurt des te meer met de doorbreking van het verwerkingsverbod op de verwerking van gezondheidsgegevens. Artikel 9, tweede lid, onder i, AVG is in de DPIA aangewezen als de toepasselijke uitzonderingsgrond. Dit artikel vereist echter dat in het lidstatelijk recht passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van de betrokkene. Hiervoor is in het wetsvoorstel Tijdelijke wet notificatieapplicatie een AMvB-bevoegdheid gecreëerd, maar deze AMvB is geen onderdeel van de aan de AP toegezonden stukken. Derhalve kan de AP niet beoordelen of voldoende tegemoetgekomen is aan deze eis van artikel 9, tweede lid, onder i, AVG.

Concluderend oordeelt de AP dat voor de gezamenlijk verwerkingsverantwoordelijken in de huidige Wpg onvoldoende grondslag voor de verwerking van (bijzondere) persoonsgegevens aanwezig is. Het voorgestelde wetsvoorstel Tijdelijke wet notificatieapplicatie is essentieel om een democratisch gelegitimeerde grondslag te creëren. De AP adviseert dat geëxpliciteerd wordt dat de in algemene termen omschreven systeemverantwoordelijkheid van de Minister (artikel 3 en 7 Wpg) voor de

[12] Zie EDPB Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, p. 7. Zie in dit verband ook: Europese Commissie, Guidance on Apps supporting the fight against Covid-19 pandemic, C2020, 2523 final.

infectieziektebestrijding met zich mee kan brengen dat daarbij een notificatie-app wordt ingezet en dat de Minister alsdan de bevoegdheid heeft om daartoe (bijzondere) persoonsgegevens te (laten) verwerken. Daarbij moeten de nodige waarborgen in de wet worden opgenomen zoals vereist is door artikel 9 van de AVG – zoals tijdelijkheid en verbod op onvrijwillig gebruik en zoals benoemd in voornoemde EDPB-guidelines.

Ten overvloede merkt de AP het volgende op. Er is onvoldoende informatie aanwezig om vast te stellen of, en zo ja, in welke mate, Google en Apple (mede) het doel en de middelen van de onderhavige verwerking bepalen. Er zijn signalen die daar op wijzen: zo hebben beide partijen bepaald dat een notificatie-app *alleen* gebruik mag maken van BLE en niet van bijvoorbeeld wifi of GPS. In paragraaf 5 wordt hier nader op ingegaan. Van belang is dat hierdoor mogelijk ook deze beide partijen ofwel een grondslag in wetgeving dienen te krijgen, ofwel verwerkers zijn, ofwel dat er met hen om andere redenen, zoals het maatschappelijk belang, afspraken gemaakt dienen te worden.

Noodzaak en effectiviteit
Door de inzet van technologie die niet eerder voor een dergelijk doel is ingezet ontbreekt op dit moment voldoende wetenschappelijk bewijs om de effectiviteit aannemelijk te maken. Om te voldoen aan dit onderdeel van de noodzakelijkheidsvereiste moet de app bij voortduring op effectiviteit worden gemonitord en moeten bij voortduring de (wetenschappelijke) inzichten uit binnen- en buitenland worden gewogen en geadresseerd. Als uit de veldtests die nog in uitvoering zijn of uitgevoerd worden blijkt dat de mate van valse positieven of valse negatieven onaanvaardbaar hoog zijn moeten die conclusies tot een daadwerkelijke herijking van de inzet van de notificatie-app leiden.

Over deze zekerheid moet de gebruiker transparant worden geïnformeerd en het moet voor de gebruiker duidelijk zijn welke mate van zekerheid hij of zij kan koppelen aan een eventuele notificatie en welke actie daarbij van de gebruiker wordt gevraagd (zoals het doen van een COVID-19-test). Uit screenshots van de app maakt de AP op dat deze informatievoorziening na het krijgen van een melding begrijpelijk is weergeven met het advies om een test aan te vragen en op basis van de fysieke klachten van de gebruiker eventueel contact op te nemen met de huisarts van de gebruiker.

Onder noodzaak valt ook de mate van proportionaliteit van de app. Dat wil zeggen: staat het middel in verhouding tot het beoogde doel? Dit hangt sterk samen met de technische inrichting van de notificatie-app, waarover hieronder meer. Ook is de proportionaliteit afhankelijk van de wettelijk vastgelegde waarborgen, zoals tijdelijkheid en een verbod op niet-verplicht gebruik, waarop de AP in haar wetgevingsadvies van 9 juni 2020 al is ingegaan.

Onder noodzaak valt tot slot ook de subsidiariteit van de notificatie-app. Dat wil zeggen: zijn er minder verstrekkende middelen om het beoogde doel te bereiken? De AP constateert dat de DPIA hier summier op ingaat, maar ziet geen aanleiding hier verder op te adviseren.

Toestemming is niet passend
Hoewel – theoretisch – de optie bestaat de expliciete toestemming van betrokkene te gebruiken als verwerkingsgrondslag (zoals vereist ex artikel 6 AVG) en als grond voor een uitzondering op het verbod op verwerking van bijzondere persoonsgegevens (zoals vereist ex artikel 9 AVG), acht de AP dit gelet op de voorziene wijze van verwerking van (bijzondere) persoonsgegevens bij de notificatie-app minder gepast.

Met hantering van toestemming als grondslag voor verwerking van persoonsgegevens is namelijk geassocieerd dat er een 'sterke' controle van betrokkene over de verwerking van diens persoonsgegevens is. Bij de voorziene wijze van verwerking van diens persoonsgegevens in de notificatie-app is intrekking van toestemming of het maken van bezwaar tegen deze verwerking echter niet tot nauwelijks realiseerbaar. Zo kan betrokkene door intrekking van een eenmaal gegeven toestemming weliswaar de verdere verzameling van persoonsgegevens voorkomen, maar kan niet na een beroep op het recht op vergetelheid (artikel 17 AVG) de verwijdering van reeds verzamelde persoonsgegevens worden bewerkstelligd. Die bevinden zich namelijk – gedurende 14 dagen na contact – in de app van andere gebruikers. Ook kan na de door de gebruiker ingevoerde melding over een coronabesmetting de gegevensverwerking via de backend server niet (meer) ongedaan worden gemaakt. Deze wordt nog minstens 24 uur na intrekking van de toestemming en/of verwijdering van de app verwerkt.

Toestemming zoals vereist in de Telecommunicatiewet

In de DPIA wordt terecht aandacht geschonken aan artikel 11.7a Telecommunicatiewet. De voorgenomen verwerking valt onder deze bepaling, nu informatie op de randapparatuur van de gebruiker wordt geplaatst of toegang wordt verkregen tot informatie in deze randapparatuur ongeacht of er sprake is van persoonsgegevens. Hiervoor is toestemming van die gebruiker vereist. De AP is van oordeel dat de gevraagde toestemming in het Google Apple Exposure Notification framework voor het activeren van BLE aan dit vereiste voldoet, mits de informatievoorziening duidelijk is in overeenstemming met het hiernavolgende over de informatieverplichtingen[13].

4.3.2 Informatieverplichtingen en de uitoefening van de rechten van betrokkenen

De informatie die krachtens de artikelen 12, 13 en 14 AVG moet worden verstrekt moet beknopt, transparant, begrijpelijk, in gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal beschikbaar worden gesteld, afgestemd op de doelgroep(en) van de verwerking.[14] Het transparantiebeginsel onderschrijft het belang van tests met verschillende doelgroepen die mogelijk op basis van fysieke of mentale beperkingen moeite hebben informatie tot zich te nemen. De AP complimenteert de Minister op dit punt met de inclusieve benadering in de ontwikkelingsfase.

De AP heeft geen documenten, zoals privacystatements, ontvangen en deze dan ook niet getoetst. Wel adviseert de AP rekening te houden met het volgende.

Uit hoofde van artikel 13 AVG dient de verwerkingsverantwoordelijke bij het verzamelen van persoonsgegevens de betrokkene te informeren over, onder andere, de identiteit en de contactgegevens van de verwerkingsverantwoordelijke of zijn of haar vertegenwoordigers, de verwerkingsdoeleinden en de rechtsgrond voor de verwerking. Het is in dit kader van belang dat de verwerkingsverantwoordelijke de betrokkene op meerdere momenten om instemming vraagt: bij het installeren van de app, het aanzetten van de BLE-functionaliteit van het Google Apple Exposure Notification framework en bij het versturen van de contactcodes. Deze instemmingen zijn echter geen toestemming in de zin van artikel 6, eerste lid, onder a, AVG, ofwel toestemming als verwerkingsgrondslag. In het kader van de effectieve uitvoering van de rechten van betrokkenen is het daarom van belang dat duidelijk is dat het geven van toestemming dus voor *andere* doeleinden (zijnde de Telecommunicatiewet) geschiedt dan de verwerking van persoonsgegevens en het intrekken van de toestemming dus niet de gevolgen heeft zoals artikel 7, derde lid, AVG omschrijft. Dit voorkomt verwarring bij de betrokkene over de grondslag voor de verwerking.

[13] Afgestemd met de Autoriteit Consument en Markt op 4 augustus 2020.
[14] Zie de Richtsnoeren inzake transparantie overeenkomstig Verordening 2016/679 (WP260rev.01) van Working Party 29, onderschreven door de European Data Protection Board op 25 mei 2018.

Nu de notificatie-app (grotendeels) gaat om decentrale opslag van persoonsgegevens, is het van groot belang om de rechten van betrokkenen op een juiste manier technisch en organisatorisch vorm te geven. Deze rechten van betrokkene (recht op inzage, recht op rectificatie, recht op gegevenswissing, recht op beperking van verwerking, kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens of verwerkingsbeperking, recht op overdraagbaarheid van gegevens en recht van bezwaar met name ook bij verwerking zoals bedoeld in artikel 6, eerste lid, onder e, AVG) moeten ook bij decentrale opslag van persoonsgegevens in lijn met de AVG worden gefaciliteerd. De AP adviseert in de afspraken tussen de gezamenlijk verwerkingsverantwoordelijken duidelijk beleid op te nemen over de omgang met de uitoefening van rechten van betrokkenen. Daarmee kan aannemelijk worden gemaakt in welke gevallen de identificatie van betrokkene voor zowel de Minister als de GGD zodanig gecompliceerd is dat een beroep op de uitzonderingsgrond van artikel 11, tweede lid, samen met artikel 12, tweede lid, AVG gerechtvaardigd is.

4.4 Technische en organisatorische maatregelen

4.4.1 Beveiliging: Beschikbaarheid, Integriteit en Vertrouwelijkheid

De genomen waarborgen, die moeten zorgen voor de beschikbaarheid van de systemen, dragen bij aan een betrouwbaar systeem en lijken toereikend voor de applicatie.

De AP ziet ook dat er afdoende maatregelen zijn getroffen die toezien op de integriteit van de gegevens. Het moedwillig manipuleren van de gegevens wordt op een adequate manier voorkomen.

De AP onderschrijft dat bij de ontwikkeling van de notificatie-app en de backend server rekening is gehouden met versleuteling bij het uitwisselen van gegevens tussen de app en de backend server. Daarnaast is er in de DPIA beschreven dat gebruik wordt gemaakt van het versturen van dummy-data om zo identificatie van een positief geteste individu, aan de hand van analyse van het netwerkverkeer te beperken.

4.4.2 Telemetrie en Google Play Services op Android

In een recent paper van onderzoekers van Trinity College wordt het risico benoemd waarbij telemetrie (op afstand meten van bepaalde parameters) over het gebruik van het Google Apple Exposure Notification framework wordt gedeeld met Google door middel van Google Play Services. [15] Het Google Apple Exposure Notification framework is geïmplementeerd binnen Google Play Services. Het is niet mogelijk om Google Play Services uit te zetten. De enige manier waarop de verzameling van telemetrie stopt is door dit uit te schakelen voor Google Play Services. Het verzamelen van telemetrie staat nu standaard ingeschakeld.

Verder plaatst de AP vraagtekens bij het ontwerp van de telemetrie in (achterliggende) onderdelen van het Exposure Notification Framework in het mobiele besturingssysteem van Google. Dit ontwerp geeft Google mogelijk inzicht in het gebruik van de app in combinatie met het framework. Zoals welke notificaties worden aangeklikt of genegeerd, maar ook metadata over onder andere het type telefoon en softwareversie.[16]

4.4.3 Bluetooth en locatiepermissies op Android

Bij het Android-besturingssysteem is het nodig toestemming te geven voor locatiebepaling om de bluetooth-functionaliteit en daarmee de notificatie-app te laten werken. Google kwalificeert het gebruik

[15] https://www.scss.tcd.ie/Doug.Leith/pubs/contact_tracing_app_traffic.pdf
[16] https://developers.google.com/android/exposure-notifications/telemetry-design, geraadpleegd op 03-08-2020.

van de bluetooth-radio in Android als het gebruik van een 'locatieservice', derhalve meent Google dat de in Android benodigde instemmings-popup voor het gebruik van de locatie van de telefoon moet worden getoond. Dit is een limitatie aan het toestemmingsraamwerk wat Google in Android hanteert en is in tegenspraak met de functionaliteit van de app en kan verwarring wekken bij de gebruiker. Uw ministerie heeft hier aandacht voor en de begeleidingscommisie adviseert de Minister om de notificatie-app pas landelijk uit te rollen zodra de onderhandelingen tot een goed einde zijn gebracht en de locatiepermissie niet meer een verplicht onderdeel is van de bluetoothpermissie. Google laat in haar blog van 31 juli 2020[17] weten dat zij een uitzondering ontwikkelen om de locatiepermissie, bij applicaties die het Google Apple Exposure Notification framework gebruiken, niet te hoeven in te schakelen. Maar deze aanpassing is alleen beschikbaar in de nieuwste Android-versie (11) en dat betekent dat deze aanpassing niet beschikbaar is voor het grootste gedeelte van de Android-toestellen.[18] Nota bene: voor veel toestellen is een update naar Android 11 überhaupt niet beschikbaar dan wel zal deze pas na maanden of soms jaren beschikbaar zijn. De AP onderschrijft het advies van de begeleidingscommissie hierover en vult daarbij aan dat het niet afdoende is dat alleen nieuwere versies van het besturingssysteem van deze uitzondering worden voorzien.

4.4.4 Kwaliteit van de broncode

Het ontwikkelteam van de notificatie-app heeft de ontwikkeling van de applicatie op een transparante manier aangepakt. Het team maakte de broncode van de app en backend server openbaar, waardoor een ieder de werking van de applicatie kan controleren. Verder is de expertise van diverse specialisten en onafhankelijke partijen ingeschakeld, onder meer voor het testen van de gebruiksvriendelijkheid en effectiviteit van de beveiligingsmaatregelen.

De AP heeft geen referenties gevonden naar externe afhankelijkheden in de broncode waarbij er gegevens over de gebruiker van de app worden gedeeld met derde partijen (afgezien van het Google Apple Exposure Notification framework) anders dan beschreven in de DPIA.

Inmiddels hebben Google en Apple (deels) de broncode van het Google Apple Exposure Notification framework vrijgegeven voor zowel Android als iOS.

Het ontwikkelteam heeft via de DPIA te kennen gegeven een hoge kwaliteit van broncode van de app en bijbehorende backend server na te streven. De AP onderschrijft dat maatregelen die zijn genoemd in de DPIA daartoe kunnen bijdragen. Bij een controle op de openbare broncode van de app en de bijbehorende backend server tijdens de beoordeling van de DPIA is echter gebleken dat de voorgenomen maatregelen nog niet volledig genomen waren. Zo ontbreekt er een overzicht van de gedraaide software-testen (bij de Apple iOS-broncode is deze inmiddels toegevoegd) en de daarbij behorende dekkingsgraad. Tevens is de rapportage van de broncode-kwaliteit niet aangetroffen in de publieke opslagplaats van de broncode (code-repository) en is de broncode summier becommentarieerd.

Daarnaast is er bij de beoordeling opgemerkt dat er geen code-review wordt gedaan in de publieke broncode. Dit draagt niet bij aan de transparantie van de ontwikkeling van de notificatie-app.

4.5 Verdere beoordeling van de voorgenomen verwerkingen en de risico's van de verwerking

De voorgenomen verwerking is nog volop in ontwikkeling, zoals ook de verwerkingsverantwoordelijken aangeven. De AP kan daarom niet op alle onderdelen een volledige beoordeling geven van de risico's. De

[17] https://blog.google/inside-google/company-announcements/update-exposure-notifications/amp/
[18] https://www.xda-developers.com/android-version-distribution-statistics-android-studio/

risico's zoals verwoord in de DPIA vallen op door de eenzijdigheid die zij weerspiegelen, het zijn vrijwel uitsluitend technische beveiligingsrisico's. Risico's voor de rechten en vrijheden van een natuurlijk persoon zijn veel diverser dan enkel de beveiliging van systemen, hoewel ook dat altijd een belangrijk onderdeel is van de verwerking van persoonsgegevens. De AP constateert dat risico's wat betreft de rechten van betrokkenen, de positionering van de FG, mogelijke internationale aspecten van de verwerking, en overeenkomsten tussen betrokken partijen niet zijn onderzocht of niet zijn weergegeven in de DPIA. De AP zal hier in de geadviseerde maatregelen en verdere adviezen op terugkomen.

De mitigerende maatregelen die de verwerkingsverantwoordelijken voorstellen (zie ook bijlage) zijn op onderdelen voldoende, waarbij de AP aantekent dat dergelijke maatregelen doorlopend vragen om onderhoud en verbetering. Het instellen van bijvoorbeeld een Plan-Do-Check-Act cyclus is hiervoor aan te bevelen. De AP geeft in hoofdstuk 6 aanvullende adviezen om de risico's beter te mitigeren. Er zijn ook maatregelen die niet te beoordelen zijn omdat de uitvoerende organisatie ontbreekt, afspraken ontbreken, of er geen of onvoldoende informatie is over een werkwijze. Dan zijn er maatregelen die de AP als onvoldoende onderbouwd of mitigerend beoordeelt. Hier ontbreken bijvoorbeeld technische of organisatorische maatregelen, ontbreken afspraken met bijvoorbeeld derde partijen zoals Google en Apple, of ontbreekt recente (technische) informatie.

5. Conclusie beoordeling voorgenomen verwerking

De AP constateert op basis van de ontvangen informatie dat de voorgenomen verwerking een samenstel van verwerkingen betreft. Voor de helderheid en volledigheid zal de conclusie op deze onderdelen van de voorgenomen verwerking ingaan. Het betreft:

- de notificatie-app software die het ministerie van VWS heeft ontwikkeld;
- de organisatorische inbedding: de wetgeving, gezamenlijke verantwoordelijkheid en waarborgen van rechten van betrokkenen;
- de backend server die ten tijde van dit advies nog niet bekend is/zijn;
- het Google Apple Exposure Notification framework, dat de technische basis voor uitwisseling van nabijheidsgegevens via Bluetooth Low Energy biedt waarop de app en de backend server functioneren.

5.1 Algemeen beeld maatregelen/risico's

De inzet van een notificatie-app heeft potentieel invloed op een zeer grote groep Nederlanders. Potentiële risico's dienen daarom op een juiste wijze verminderd of weggenomen te worden. De DPIA laat zien dat vooral wat de beveiliging van de persoonsgegevens in de notificatie-app zelf veel maatregelen genomen zijn. Dit is positief, en dient ook tijdens de verwerking scherp gemonitord te worden. Risico's voor betrokkenen zijn echter breder dan de beveiliging van systemen, software of communicatie.

Wanneer een gebruiker van de notificatie-app bericht krijgt van mogelijke blootstelling aan een besmet persoon, vermeldt de notificatie-app tevens op welke dag dit is geweest. De AP begrijpt dat dit noodzakelijk kan zijn om doeltreffend actie te kunnen ondernemen als persoon en als gezondheidsdienst, maar dit kan wel resulteren in de herleiding tot een besmet persoon. Als het contact bijvoorbeeld op een dag is geweest waarom de gebruiker maar met één persoon lang genoeg in contact is geweest, dan is de

herleiding simpel. Hoewel dit risico mogelijk niet volledig weggenomen kan worden, komt dit ook niet terug in de DPIA. De AP zal bij de adviezen hier verder op ingaan.

Tevens valt op dat bij een aantal risico's een wetsartikel wordt aangehaald als maatregel. De AP merkt hierover op dat het enkele bestaan van bijvoorbeeld een verbod op verwerking van persoonsgegevens op zichzelf geen technische of organisatorische maatregel onder de AVG kan zijn. Het kan wel een sluitstuk vormen van een maatregel waarin ook detectie of toezicht wordt toegepast.

5.2 De notificatie-app software

Het 'privacy-by-design'-principe is een belangrijk onderdeel van de AVG. Door verwerkingen al in de ontwerpfase zo privacyvriendelijk mogelijk vorm te geven worden de gegevensstromen geminimaliseerd, de beveiliging geoptimaliseerd, en de rechten en vrijheden van natuurlijke personen maximaal gerespecteerd. De AP constateert met genoegen dat de notificatie-app software zich aan het 'privacy-by-design'-principe heeft gecommitteerd. Er is zichtbaar nagedacht over de wijze waarop de app functioneert en interacteert met de andere onderdelen van het samenstel van verwerkingen. De gegevensstromen zijn minimaal, de mate van herleidbaarheid wordt geminimaliseerd, en er zijn goede beveiligingsmaatregelen getroffen in het ontwerp. De AP concludeert op grond van de ontvangen informatie dat er geen inbreuk op de AVG plaatsvindt binnen de notificatie-app software als sub-onderdeel van het stelsel van verwerkingen. Wel wil de AP benadrukken dat de notificatie-app software onderdeel moet zijn van een continue cyclus van monitoring en verbetering (PDCA-cyclus). Mogelijke problemen moeten snel geïdentificeerd en verholpen worden, verbeteringen moeten zo snel mogelijk worden doorgevoerd, en de beveiliging dient doorlopend te worden bijgehouden. De AP geeft in hoofdstuk 6 hiervoor een aantal adviezen.

5.3 Wetgeving en organisatorische inbedding

De notificatie-app software en de backend server vallen onder de verantwoordelijkheid van de Minister van VWS en de GGD'en. Hiervoor zijn drie randvoorwaarden van belang die de AP hier zal behandelen: de wetgeving die een grondslag biedt voor deze voorgenomen verwerking, de afspraken tussen de gezamenlijk verwerkingsverantwoordelijken, en het organiseren en waarborgen van de rechten van betrokkenen.

De AP is van oordeel dat de voorgenomen verwerking van persoonsgegevens in beginsel geen rechtmatige grondslag heeft, omdat de Minister, als gezamenlijk verwerkingsverantwoordelijke met de 25 GGD'en, onvoldoende grondslag voor de verwerking van (bijzondere) persoonsgegevens heeft in artikelen 3 en 7 van de Wpg. Dit zal in de vorm van aanvullende tijdelijke wetgeving moeten worden geregeld. Hiervoor merkt de AP het volgende over op: deze wetgeving dient een heldere en expliciete grondslag te geven voor de verantwoordelijke partijen voor deze specifieke verwerking. Kortom: de wetgeving moet de in het verzoek als gezamenlijk verwerkingsverantwoordelijke genoemde partijen expliciet benoemen en een grondslag geven, en die grondslag moet ook expliciet de in het verzoek genoemde voorgenomen verwerking betreffen. Om de benodigde uitzondering op de verwerking van bijzondere persoonsgegevens te rechtvaardigen, zullen in die wetgeving de benodigde waarborgen, zoals onder andere tijdelijkheid, (waaronder de exit-strategie) en vrijwilligheid (waaronder het verbod op onvrijwillig gebruik) voldoende moeten worden geadresseerd. Pas dan is er voldoende grondslag voor de verwerking van (bijzondere) persoonsgegevens.

De gezamenlijk verwerkingsverantwoordelijken dienen onderling afspraken te maken en vast te leggen over de verdeling van taken, omgang met persoonsgegevens, en de waarborgen voor betrokkenen.

Betrokkenen moeten hun rechten kunnen uitoefenen voor de persoonsgegevens die in de voorgenomen verwerking worden verwerkt. Hier mogen geen onredelijke belemmeringen bestaan, er moet een goede contactmogelijkheid bestaan, en de betrokkenen moeten worden voorzien van heldere en neutrale informatie over de verwerking. Ook dit moeten de gezamenlijk verwerkingsverantwoordelijken nog vormgeven.

5.4 Backend server

Tijdens de behandeling van dit verzoek bevestigde de Minister dat de organisatie die de backend server zou hosten (de Belastingdienst) zich heeft teruggetrokken. Een nieuwe organisatie die dit onderdeel van het samenstel van verwerkingen faciliteert is ten tijde van dit advies nog niet bevestigd; de AP kan dit onderdeel daarom niet beoordelen. De AP constateerde dat de maatregelen die getroffen waren door de Belastingdienst, zoals omschreven in de DPIA, voldoende waarborgen boden voor de inzet in de voorgenomen verwerking. Een nieuwe organisatie zal tevens aan deze standaarden moeten voldoen.

5.5 Google Apple Exposure Notification framework

De technische basis voor uitwisseling van nabijheidsgegevens via Bluetooth Low Energy waarop de app en de backend server functioneren wordt door Google en Apple ontwikkeld en beheerd in het kader van de bestrijding van COVID-19. Deze is ingebouwd in de mobiele besturingssystemen Android en iOS.
De Minister heeft ervoor gekozen het Google Apple Exposure Notification framework in te zetten. Naast de technische aanpassingen die Google en Apple hebben gedaan om contactmomenten middels Bluetooth beter te kunnen detecteren, bevat het Google Apple Exposure Notification framework aanvullingen op het normale besturingssysteem van een telefoon die mogelijk wenselijk zijn bij die bestrijding van Covid-19, maar die niet kunnen worden gezien als logische technische aanpassingen binnen de normale werking van een telefoon. Dit komt mede tot uiting in de fasering die door Google en Apple is voorzien.

In de eerste fase van de ontwikkeling van het Google Apple Exposure Notification framework kan dit framework niet zonder de app en kan de app niet zonder het framework. Deze nauwe verbondenheid maakt het succes van deze oplossing dan ook afhankelijk van een zeer goede samenwerking tussen het Google Apple Exposure Notification framework en de nationale app. Google en Apple hebben dan ook strikte (technische) voorwaarden gesteld voor het mogen gebruiken van het framework van Google en Apple. In de tweede fase van het Google Apple Exposure Notification framework gaat deze meer activiteiten zelfstandig uitvoeren en is de nu ontwikkelde app van het ministerie van VWS niet langer noodzakelijk. Zoals eerder aangegeven gaat dit advies alleen over de verwerkingen gerelateerd aan de eerste fase van het Google Apple Exposure Notification framework.
Op basis van de ontvangen en bekende informatie kan de AP geen beeld vormen van het Google Apple Exposure Notification framework. Het is onvoldoende duidelijk of, en zo ja welke, persoonsgegevens worden verwerkt door Google en Apple middels het aanbieden van het framework. Ook is onduidelijk of Google en Apple (mede) het doel en middelen van de verwerking bepalen en daarmee (mede) verwerkingsverantwoordelijke zijn. De verwerkingsverantwoordelijken dienen heldere en sluitende afspraken te maken met Google en Apple waarin vastgelegd wordt wat door Google en Apple wel en niet verwerkt wordt of mag worden, welke waarborgen daarvoor bestaan, en bij eventuele verwerkingen een DPIA of aanvullend een voorafgaande raadpleging eventueel nodig is. In de huidige documentatie verwijst de Minister enkel naar een online Frequently-Asked-Questions pagina, een levend document dat éénzijdig gewijzigd kan worden en waaraan geen enkele rechten of waarborgen ontleend kunnen worden. Waarborgen en voorwaarden betreffende de werking, aanpassing en het gebruik van het framework dienen contractueel vastgelegd te worden. Het ontbreken van afspraken en waarborgen biedt onvoldoende zekerheid om rechtmatig met de verwerking als geheel van start te kunnen gaan.

Op grond van de ontvangen informatie en het voorgaande concludeert de Autoriteit Persoonsgegevens dat de voorgenomen verwerking COVID-19 notificatie-app zoals beschreven ten minste inbreuk zou maken op artikelen 5, 6, 9, 32 en 35 van de AVG.

6. Maatregelen

Teneinde te waarborgen dat u met de voorgenomen verwerking niet de AVG overtreedt, adviseert de AP, gelet op haar bevoegdheid als bedoeld in artikel 58, derde lid, onder a, en tweede lid, onder a, van de AVG als volgt.

Ten aanzien van de risico's van de voorgenomen verwerking geeft de Autoriteit Persoonsgegevens aan dat de volgende maatregel(en) noodzakelijk zijn om door te voeren voordat de verwerking zal starten:

6.1 Google Apple Exposure Notification framework

De gezamenlijk verwerkingsverantwoordelijken dienen middels een overeenkomst afspraken vast te leggen betreffende de werking van het framework, eventuele verwerkingen van (persoons)gegevens en toekomstige ontwikkelingen van het framework die van invloed zijn op de werking van het framework, of de uitwerking daarvan voor de betrokkenen in Nederland. Concreet adviseert de AP de volgende maatregelen ten aanzien van het Google Apple Exposure Notification framework:

1. Schriftelijke contractuele afspraken te maken met Google en Apple[19], in lijn met mogelijk al bestaande afspraken op Rijksniveau, aangaande de werking van het Google Apple Exposure Notification framework in fase 1. Dit omhelst ook garanties en waarborgen aangaande de stelling van Google en Apple dat zij geen persoonsgegevens verwerken of gaan verwerken in het Google Apple Exposure Notification framework.
2. Heldere afspraken te maken over het moment waarop het ministerie van VWS de werking van de app beëindigt en de wijze waarop op dat moment de toepassing van het Google Apple Exposure Notification framework ook wordt gestopt.
3. Heldere afspraken te maken over de vraag of, en zo ja, welke gegevens door Google en Apple dienen te worden verwijderd indien de voorliggende verwerking in de toekomst wordt gestaakt.
4. Te bepalen of, en zo ja, onder welke condities het wenselijk is dat fase 2 van het Google Apple Exposure Notification framework überhaupt in Europa c.q. Nederland wordt ingezet. Daarbij dient dan tevens aandacht te worden geschonken aan de vraag wie in die fase verwerkingsverantwoordelijk is en dient de mogelijke DPIA/VR-plicht te worden benadrukt. Mede in het licht van het eerder uitgevoerde ethisch assessment is het wenselijk om een beeld te vormen over de wenselijkheid dat het zwaartepunt van de oplossing nog meer verschuift naar het Google Apple Exposure Notification framework. De Minister heeft daar in die fase mogelijk minder of zelfs helemaal geen invloed meer op. Bezien vanuit het feit dat het de Minister is die hier de publieke en wettelijke taak heeft tot bestrijding van infectieziekten en deze taak niet is voorzien te worden uitgevoerd door private marktpartijen.

6.2 Wetgeving en organisatorische inbedding

Zonder passende wetgeving is de introductie van de notificatie-app niet mogelijk. De AP adviseert om passende tijdelijke wetgeving aan de wetgever voor te stellen waarin een heldere en expliciete grondslag

[19] Zijnde: Google LLC (1600 Amphitheatre Parkway, Mountain View, California 94043, United States) en Apple INC. (1 Apple Park Way in Cupertino, California, United States).

wordt gegeven voor zowel de verantwoordelijke partijen als de specifieke verwerking. Ook is het van belang dat het gebruik van de notificatie-app vrijwillig is, en dat verplichting hiervan ook bij wet wordt verboden.
Tevens adviseert de AP om heldere afspraken te maken tussen de gezamenlijk verwerkingsverantwoordelijken over de verdeling van taken, omgang met persoonsgegevens, en de waarborgen voor betrokkenen. Ook de uitoefening van de rechten van betrokkenen dient vastgelegd te worden in afspraken tussen de gezamenlijk verwerkingsverantwoordelijken.

6.3 Backend server

Vanwege het ontbreken van een organisatie die de backend server host, zal de AP hier enkel kort ingaan op de situatie die voor de in de DPIA vermelde organisatie geldt. De standaarden betreffende technische en organisatorische maatregelen zoals vermeld in de DPIA waren voldoende voor de voorgenomen verwerking. Ook bij een nieuwe organisatie zullen de verwerkingsverantwoordelijken voldoende technische en organisatorische maatregelen moeten vastleggen om te voldoen aan de hoge standaarden die voor een verwerking als deze gelden. Vanzelfsprekend dient hier een verwerkersovereenkomst (artikel 28, derde lid van de AVG) te worden afgesloten. Dit geldt niet enkel voor de beveiliging, maar tevens voor de organisatorische maatregelen die waarborgen moeten bieden wanneer (bijzondere) persoonsgegevens worden verwerkt. Na de start van de verwerking dienen de verwerkingsverantwoordelijken de maatregelen te monitoren en waar nodig te versterken.

7. Verdere adviezen

Naast de bovenstaande maatregelen die noodzakelijk zijn om door te voeren voor de start van de verwerking geeft de AP ook aanvullende adviezen die in acht moeten worden genomen bij de voorgenomen verwerking van persoonsgegevens.

7.1 Juridisch

Het inzetten van een app met het bijbehorende samenstel van verwerkingen voor bron- en contactonderzoek is een verregaande maatregel die, gezien de huidige situatie, enkel tijdelijk van aard kan zijn en enkel kan worden ingezet indien de situatie op dat moment een dergelijke maatregel vereist. In de DPIA is de tijdelijkheid van deze maatregel niet geadresseerd. De AP adviseert een wettelijke einddatum voor de verwerking vast te leggen en vast te leggen onder welke voorwaarden een verlenging door de wetgever mogelijk is.

Zorg voor een volledige en juiste DPIA voor de start van de verwerking, en pas deze waar nodig aan indien tijdens de verwerking wijzigingen worden doorgevoerd. De DPIA dient alle onderdelen van de verwerking te omvatten, en bijvoorbeeld ook overeenkomsten betreffende rechten van betrokkenen, en tussen alle betrokken partijen te bevatten. Deze verwerking is DPIA-plichtig. Het Besluit lijst verplichte DPIA[20] geeft hiervoor negen criteria uit de Europese richtsnoeren, waarbij de AP constateert dat de voorgenomen verwerking aan voldoende van deze criteria voldoet om voor de DPIA-plicht in aanmerking te komen. Verder duidt de AP in het Besluit ook aanvullende specifieke verwerkingen aan waarvoor een DPIA verplicht is. Op deze lijst staat onder andere ‘observatie en beïnvloeding van gedrag’, waar deze verwerking onder andere aan voldoet. Dit betekent dat voor de start van de voorgenomen verwerking een volledige DPIA moet zijn opgesteld voor alle onderdelen van de verwerking. Die moet zijn ondertekend door de verwerkingsverantwoordelijken en de FG’s moeten hierop een advies hebben uitgebracht.

[20] Zie hiervoor de website van de AP: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia

Omdat dit een voorgenomen verwerking betreft waarvoor een DPIA-plicht geldt, dient de verwerkingsverantwoordelijke voorafgaand aan de verwerking de betrokkenen of hun vertegenwoordigers om hun mening te vragen ingevolge artikel 39, negende lid AVG.

7.2 Organisatorisch

De taken en verantwoordelijkheden van de verwerkingsverantwoordelijken dienen te worden vastgelegd in afspraken tussen de betrokken partijen. De AP adviseert deze afspraken conform artikel 26 AVG voorafgaand aan de start van de verwerking vast te leggen.

Voor een juiste uitoefening van rechten van betrokken is het van belang dat de betrokken FG's juist gepositioneerd zijn binnen de organisatie en voorzien zijn van voldoende middelen om hun functie uit te oefenen. Dit kan onderdeel zijn van de afspraken tussen de verwerkingsverantwoordelijken om te zorgen dat er geen belemmeringen ontstaan voor de uitoefening van de rechten van betrokkenen.

7.3 Technisch

De AP adviseert de risico's met betrekking tot verwevenheid van het Google Apple Exposure Notification framework met Google Play Services te onderzoeken en afspraken te maken met Google om dit risico te mitigeren. Hierbij verdient met name de mogelijkheid van telemetrie door Google bijzonder de aandacht. Daarnaast dient nader te worden onderzocht op welke wijze Android-telefoons zonder Google Play Services gebruik kunnen maken van de notificatie-app.

De AP stelt vast dat het team achter DP3T gegevensbeschermingsverbeteringen heeft doorgevoerd aan het systeem die nog niet door Google en Apple in het Google Apple Exposure Notification framework zijn opgenomen. Specifiek doelt de AP dan op:

- De aanbeveling om een TEK maximaal 2-4 uur geldig te laten zijn in plaats van 24 uur;
- De techniek 'shared secrets' toepassen op het uitzenden van RPI's.

De AP adviseert deze verbeteringen mee te nemen in de doorontwikkeling van de notificatie-app.

Verder adviseert de AP:

- In navolging van de begeleidingscommissie de verwerkingsverantwoordelijken in het kader van de transparantieverplichtingen om Google op te dragen de eis tot toestemming tot 'locatieservices' te schrappen en de functionaliteit niet als locatieservice aan de gebruiker te tonen;
- Te onderzoeken of het uitschakelen van de mogelijkheid om screenshots te maken in de notificatie-app kan bijdragen aan een mogelijke vermindering van het risico op onvrijwillig gebruik van de notificatie-app;
- Voor zover technisch mogelijk zogenaamde *reproducible builds* van de Android- en iOS-app te publiceren;
- Overzichten van gedraaide software-testen en code reviews en hun uitslag te publiceren, inclusief bijbehorende dekkingsgraad;
- Uitgebreidere becommentariëring van de broncode door de ontwikkelaars.

8. Conclusie advies op voorafgaande raadpleging

ADVIES:
De Autoriteit Persoonsgegevens adviseert u om niet starten met de voorgenomen verwerking voordat de bovengenoemde maatregelen zijn getroffen en de adviezen van de Autoriteit Persoonsgegevens in acht zijn genomen.

In het geval dat de verwerking in de praktijk wezenlijk anders is dan uit de overgelegde stukken blijkt en waarop dit advies is gebaseerd, of dat een gewijzigde/nieuwe werkwijze leidt tot een wezenlijk andere verwerking dan waarop dit advies ziet, dient u te beoordelen of u de gewijzigde respectievelijk nieuwe verwerking opnieuw dient te beoordelen ingevolge artikel 35 van de AVG en eventueel op grond van artikel 36, eerste lid van de AVG opnieuw dient te verzoeken om voorafgaande raadpleging. Op basis van artikel 58 van de AVG kan de AP guidance-afspraken ten aanzien van de verwerking vastleggen met de FG en verwerkingsverantwoordelijken.

Deze beoordeling laat onverlet dat klachten of andere informatie over de verwerking er alsnog toe kunnen leiden dat de AP nadere inlichtingen inwint of een onderzoek start. De AP kan ook ambtshalve om informatie verzoeken betreffende de verwerking of een onderzoek starten naar (onderdelen van) de verwerking.

Mochten er naar aanleiding van dit advies vragen zijn, dan kunt u die aan de contactpersoon richten.

Hoogachtend,
Autoriteit Persoonsgegevens,
Namens deze,

Directeur Systeemtoezicht, beveiliging en technologie

AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Vragen over de Algemene verordening gegevensbescherming

Op onze website autoriteitpersoonsgegevens.nl vindt u informatie en antwoorden op vragen over de Algemene verordening gegevensbescherming (AVG). Heeft u op deze website geen antwoord op uw vraag gevonden? Dan kunt u contact opnemen met het Informatie- en Meldpunt Privacy van de Autoriteit Persoonsgegevens op 088-1805 250.