AUTORITEIT
PERSOONSGEGEVENS

20 april 2020

Onderzoeksrapportage bron- en contactopsporingsapps

Inhoudsopgave

1. Aanleiding

Het Outbreak Management Team (OMT), het Nederlands adviesorgaan dat de minister van Volksgezondheid, Welzijn en Sport (VWS) en de Ministeriële Commissie Crisisbeheersing (MCCb) adviseert bij de bestrijding van een epidemie, heeft op 6 april 2020 gevraagd om digitale oplossingen die kunnen worden ingezet voor de bestrijding van het coronavirus in Nederland.

Op 11 april 2020 heeft het ministerie van VWS bedrijven en deskundigen uitgenodigd om voorstellen in te dienen voor slimme digitale oplossingen, zoals apps, die kunnen bijdragen aan bron- en contactopsporing, waarbij stringente eisen worden gesteld aan onder meer snelle beschikbaarheid, privacy en informatiebeveiliging. Voorstellen konden worden aangeleverd tot 14 april 2020.[1] Na de uitnodiging zijn meer dan 700 reacties ontvangen, waarvan 660 daadwerkelijk een voorstel bevatten.[2] Het ministerie heeft na advies van diverse deskundigen zeven inzendingen geselecteerd, die hun voorstel nader konden toelichten op 18 en 19 april 2020. Het ministerie van VWS heeft ook de Autoriteit Persoonsgegevens (AP) gevraagd om te beoordelen of de opzet van elk van de zeven apps in Nederland in overeenstemming zou zijn met de AVG.[3] Hiertoe heeft de AP op 17 april 2020 via het ministerie van VWS documentatie ontvangen over de zeven door het ministerie geselecteerde voorstellen. De documentatie die op 17 april was ontvangen was voor vrijwel alle voorstellen niet in één keer compleet. Om die reden heeft de AP ook op 18 en 19 april 2020 nog documenten ontvangen via het ministerie van VWS.

Enkele uitgangspunten zijn volgens de minister dat de inzet van digitale hulpmiddelen noodzakelijk, effectief en proportioneel is en voldoet aan bestaande wetgeving, zoals de Algemene verordening gegevensbescherming (AVG). De minister heeft aan de Tweede Kamer gemeld dat de AP als toezichthouder betrokken wordt.

Hierbij komt de AP tegemoet aan het verzoek van het ministerie van VWS. De AP benadrukt dat het aan VWS en de leveranciers is om aan te tonen dat de apps voldoen aan de geldende wet- en regelgeving omtrent gegevensbescherming. Dit volgt uit de AVG ('verantwoordingsplicht', artikel 5, lid 2, AVG). De AP toetst of dat het geval is.

2. Opzet onderzoeksrapportage

In deze onderzoeksrapportage beschrijft de AP de wijze waarop zij de opzet van de apps heeft beoordeeld. Hierbij wordt niet verwezen naar afzonderlijke apps. Enerzijds omdat de AP tot de slotsom is gekomen dat op grond van de beschikbare informatie geen oordeel kan worden geformuleerd over de vraag of de apps voldoen aan de kaders die de privacywetgeving stelt. Anderzijds omdat een deel van de informatie die aan de AP is verstrekt bedrijfsvertrouwelijk is.

[1] https://www.rijksoverheid.nl/onderwerpen/coronavirus-app/nieuws/2020/04/11/oproep-om-mee-te-denken-over-apps
[2] https://www.rijksoverheid.nl/onderwerpen/coronavirus-app/nieuws/2020/04/17/zeven-apps-doen-mee-aan-publieke-test-komend-weekend
[3] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-toetst-opzet-corona-apps. De werking van de app of apps zal later worden onderzocht, áls het kabinet daadwerkelijk kiest voor de inzet van een corona app.

3. Bevindingen AP

De AP spreekt haar waardering uit voor het innovatief vermogen van app-ontwikkelaars waarvan de AP een voorstel heeft ontvangen. Tegelijkertijd constateert de AP dat de voorstellen qua opzet nog onvoldoende uitgekristalliseerd zijn. Ook was een deel van de documenten met informatie waarop de AP zou moeten toetsen niet aanwezig, gefragmenteerd, onvolledig, laat ingediend en in verschillende talen opgesteld. Daarom komt de AP tot de volgende bevindingen:

De AP kan geen oordeel geven over de opzet van de zeven 'corona-apps' die het ministerie van VWS heeft geselecteerd. De AP vindt dat het ministerie van VWS de kaders niet duidelijk genoeg heeft gesteld. Daardoor zijn de zeven app-voorstellen onvoldoende uitgewerkt om te kunnen beoordelen of de bescherming van gevoelige gegevens van Nederlanders voldoende is gewaarborgd.

Kaders apps onduidelijk
Uit de analyse van de AP blijkt dat de kaders die de overheid stelt voor de corona-app onduidelijk zijn: in het programma van eisen voor de app is een aantal fundamentele vragen onvoldoende beantwoord.

Zo is niet duidelijk omschreven wat het doel is van de app en wie verantwoordelijk is voor de verwerking van de gegevens. Is dat een private partij, een zorgpartij of een overheid? Ook staat in het programma van eisen niet genoemd of de app een onderdeel is van een pakket aan maatregelen en welke maatregelen dat dan zijn. Terwijl het ontwerp en de werking van een app zeer afhankelijk zijn van die overige maatregelen.

Bij een ingrijpend middel als zo'n corona-app moet de AP bovendien kunnen toetsen of de inzet ervan in verhouding staat tot de mogelijke privacyschendingen. Het moet duidelijk zijn waarom alternatieven die minder ingrijpend zijn dan een app minder effectief zijn om het virus in te dammen. Dat is nu onvoldoende duidelijk. De AP kan de proportionaliteit van de inzet van de corona-apps daardoor niet beoordelen.

Te weinig informatie over apps
Het feit dat de kaders onvoldoende duidelijk zijn, maakt dat veel app-ontwikkelaars nog zoekende zijn en zij hun plannen onvoldoende hebben kunnen uitwerken, zowel op technisch als op juridisch vlak. De AP heeft van de app-ontwikkelaars te weinig informatie ontvangen om een goed beeld te krijgen van de opzet van hun apps.

Zo leverden sommige app-ontwikkelaars alleen informatie over hoe de app eruit ziet voor gebruikers, en laten ze informatie over hoe de app 'aan de achterkant' werkt achterwege. Daardoor is door de app-ontwikkelaars onvoldoende aangetoond dat de privacy technisch maar ook organisatorisch gezien gewaarborgd is.

Daarnaast onderbouwen de ontwikkelaars van de apps in hun voorstellen niet of onvoldoende waarom ze een bepaalde techniek inzetten en wat de beperkingen van die techniek zijn. Bijvoorbeeld de inzet van Bluetooth in een app die contact tussen mensen bijhoudt. Het gebruik van deze techniek kan betekenen dat er veel vals positieven zijn. De onderbouwing van dit soort keuzes is nodig voordat de AP een oordeel kan vellen.

Wanneer de noodzaak, de kaders, de plannen en de apps beter uitgewerkt zijn, kan de AP pas een afgewogen oordeel vellen.

4. Onderzoek

4.1 Opzet onderzoek

Het onderzoek naar waarborgen van de apps op het punt van gegevensbescherming, vond plaats op vrijdag 17, zaterdag 18 en zondag 19 april. De AP heeft voor de beoordeling een multidisciplinair team ingezet, bestaande uit technologen, sociaal wetenschappers en juristen. Het team heeft de voorstellen en de bijbehorende documentatie over voorgelegde apps onderzocht op zowel technische als juridische aspecten van het gegevensbeschermingsrecht. De apps zelf en de softwarecode zijn slechts zijdelings bij het onderzoek betrokken. Voor een beoordeling hiervan verwijst de AP naar het KPMG onderzoek.[4]

De AP heeft via het ministerie van VWS bij de app-ontwikkelaars de volgende documentatie opgevraagd:

1. Het verwerkingenregister*
2. De DPIA*
3. Technische documentatie over opzet en werking van de app, opslag van data en informatiebeveiliging.
4. Eventuele expertrapportages (oordelen van deskundigen, contra-expertise rapportages, evaluaties, technische testrapporten, et cetera)
5. De duidelijke handleiding en instructie*
6. Beschreven aandacht voor vertrouwelijkheid en integriteit*
7. Beschrijving van controleerbaarheid van daadwerkelijk gebruikte oplossing*
8. Omschreven doel en doelgroep*
9. Eventueel uitgevoerde audits*
10. Documentatie waaruit volgt dat wordt voldaan aan de ISO-normen*
11. Alle overige documentatie waarvan de ontwikkelaar / aanbieder denkt dat die relevant is in het kader van de vraag welke gegevensbeschermingsrisico's gepaard gaan met het gebruik van de app.
12. Contactgegevens voor aanvullende (technische en juridische gegevensbeschermingsgerelateerde) vragen.
13. Een overzicht per app van de bij die app aangeleverde documenten.

* Deze documenten maakten ook onderdeel uit van de uitvraag van het ministerie van VWS[5]

Ook heeft het ministerie van VWS een samenvatting van de opmerkingen van de door hen ingeschakelde experts aan de AP verstrekt. Eventueel online beschikbare informatie over de apps is door de AP niet meegenomen of slechts zijdelings bij de technische beoordeling betrokken. Wel heeft de AP kennis genomen van de pitches die door de app-ontwikkelaars zijn gegeven op 18 en 19 april tijdens de door het ministerie van VWS georganiseerde appathon. Ook volgden enkele AP-medewerkers is de appathon via de livestream.
Ten slotte heeft de AP twee documenten van het ministerie van VWS ontvangen over de juridische inbedding van de apps, te weten de notitie 'Uitwerking grondslag en juridische inbedding apps VWS/WJZ/ Landsadvocaat 17 april 2020' en het 'Aanbouwdocument juridische verantwoording corona-apps' van de landsadvocaat van 18 april 2020.

[4] https://www.rijksoverheid.nl/onderwerpen/coronavirus-app/documenten/publicaties/2020/04/19/rapportage-veiligheidstest-potentiele-corona-apps
[5] Document "Uitnodiging slimme digitale oplossingen Corona" via https://www.tenderned.nl/tenderned-tap/aankondigingen/192421;section=2

4.2 Opzet juridisch onderzoek

Voor de vraag of de verwerkingen van persoonsgegevens middels de voorgestelde app binnen de kaders van de AVG zouden kunnen plaatsvinden heeft de AP allereerst per app in kaart gebracht welke gegevens binnen de app zelf zouden worden verzameld, en welke gegevens vanuit de app via een centrale server met andere partijen (bijvoorbeeld de GGD) worden uitgewisseld. Hieruit bleek dat alle apps – in ieder geval in potentie – persoonsgegevens verwerken en uitwisselen. Daarnaast worden in veel gevallen ook gezondheidsgegevens verwerkt. De AVG is derhalve van toepassing op alle aan de AP voorgelegde corona-apps.
Op basis van de aangeleverde informatie heeft de AP vervolgens – voor zover mogelijk op basis van de aangeleverde informatie – een inschatting gemaakt of en hoe per app aangetoond ('aantoonplicht') wordt of aan de beginselen van rechtmatigheid, behoorlijkheid, transparantie en minimale gegevensverwerking wordt voldaan.

Opvallend genoeg ontbrak een (adequaat) verwerkingenregister in alle gevallen. Bij sommige voorstellen was door de leverancier van de app een gegevensbeschermingseffectbeoordeling[6] (op hoofdlijnen) toegevoegd. Echter door de vele nog openliggende keuzes met betrekking tot het doel van de apps, de wijze waarop de apps organisatorisch worden ingezet, de precieze functionaliteit die daaruit volgt en de te nemen beveiligingsmaatregelen van de corona-app in Nederland, waren deze DPIA's – voor zover aanwezig - weinig concreet en daarmee onvoldoende bruikbaar voor de AP om haar beoordeling op te baseren. De beschrijving van de functionele en technische werking van de verschillende apps verschilde in kwaliteit. Sommige apps waren gebaseerd op apps die al in andere landen in gebruik zijn (bijvoorbeeld in Tsjechië en in Oostenrijk) en sommige apps zijn nog in de ontwikkel- en testfase.

4.3 Opzet technisch onderzoek

Het technisch onderzoek door de AP bestond uit het analyseren van de technische documentatie.

Beschikbare gegevens

In de aan de AP aangeleverde documentatie ging het veelal om mock-ups en andere documenten met ideeën ten aanzien van te ontwikkelen apps. Bij sommige was duidelijk welke onderliggende techniek men voor de betreffende app wilde gaan gebruiken en hoe deze techniek zou moeten worden geïmplementeerd maar bij andere voorstellen was dit niet het geval. Aan de AP zijn ook geen demo's, films of ander materiaal ter beschikking gesteld. De –in een later stadium door een aantal partijen ter beschikking gestelde –broncodes zijn niet door de AP getoetst.

Appathon

Enkele AP-technologen hebben de gevolgd via de livestream. Opvallend was dat er via de appathon op beide dagen aanvullende informatie werd verstrekt die niet was opgenomen in de door de AP ontvangen documentatie. Zo kon de bij de appathon getoonde nieuwe informatie bij een aantal apps meer helderheid geven over de slechts in beperkte mate beschikbaar gestelde informatie, bijvoorbeeld informatie over onder de app ten grondslag liggende technologie of brachten zij risico's aan het licht ten aanzien van bijvoorbeeld het gebruik van telefoonnummers. In een enkel geval leek de app-ontwikkelaar gedurende de appathon te wisselen van de onderliggende techniek, dit zorgde voor verwarring ten aanzien van de analyse van de door de app-ontwikkelaar gebruikte techniek.

Inhoudelijke analyse

De AP heeft voor de technische analyse gebruik gemaakt van een vaste werkwijze, die voor elk van de apps is doorlopen. Daarbij is gekeken naar de volgende onderwerpen:

[6] Ook wel bekend als Data Protection Impact Assessment (DPIA).

- **Algehele indruk**: hierbij is globaal gekeken in hoeverre is voldaan aan AVG-principes zoals privacy by design en privacy by default.
- **De aard van de gekozen oplossing**: de gekozen oplossing; op welke wijze is de betreffende app ontworpen om het bron- en contactonderzoek uit te voeren. Bijvoorbeeld door middel van het gebruik van bluetooth of locatiegegevens, de door de app vereiste app-machtigingen, het gebruik van unieke identifiers, maar ook het gebruik van een centrale of decentrale server.
- **De software:** de door de app-ontwikkelaars gekozen software. Bijvoorbeeld of de software open-source is, of deze afhankelijk is van Software Development Kits van derden, het gebruik van privacy enhancing technologies, de distributiewijze van de app, maar ook de documentatie bij de software.
- **De beveiliging van de app**: de beveiliging van de app en de met de app verkregen gegevens. Bijvoorbeeld op welke wijze de data zelf opgeslagen en beveiligd worden en wie vervolgens bij die data kan. Speciale aandacht is besteed aan vragen die zien op het voorkomen van fraude; welke maatregelen hebben de leveranciers genomen tegen het spoofen van unieke identificatienummers, het de-anomiseren daarvan of het aanpassen van de status van een gebruiker indien iemand besmet is.

Zoals eerder aangegeven was niet alle informatie beschikbaar en konden hierdoor vragen in voorkomende gevallen niet beantwoord worden. Daar waar mogelijk is geprobeerd verder te kijken dan de door de app-ontwikkelaars aangeleverde stukken, bijvoorbeeld door het bestuderen van de onderliggende techniek. Dit kon alleen in die gevallen waar geen enkel misverstand bestond over welke onderliggende techniek het ging.

Steekproefsgewijs en in duo's hebben de betrokken onderzoekers elkaars bevindingen getoetst.

5. Bevindingen op hoofdlijnen

5.1 De noodzakelijkheid van apps niet aangetoond

Voorop staat dat de inzet van contact tracing apps een vergaande en zeer ingrijpende inbreuk oplevert op het grondrecht op privéleven van burgers. Daar komt bij dat het hier gaat om de verwerking van gegevens over gezondheid. Dat zijn zeer gevoelige (bijzondere) persoonsgegevens, waarop soms ook het medisch beroepsgeheim van artsen rust. De AP is zich overigens bewust van het algemene belang van de bescherming van de volksgezondheid en de bestrijding van infectieziekten. Dat raakt ook aan andere grondrechten van burgers, zoals het recht op leven. Idealiter zijn grondrechten met elkaar in balans. Er moet onderbouwd worden hoe de verschillende grondrechten tegen elkaar zijn afgewogen. Kernvraag vanuit het gezichtspunt van de AP is wat de noodzaak is voor een vergaande en ingrijpende inbreuk op het grondrecht op privéleven van burgers. Op het punt van de noodzaak en de effectiviteit heeft de AP in het onderzoek geen documentatie aangetroffen.
Voor de volledigheid merkt de AP op dat die noodzakelijkheid er ook moet zijn indien de app op basis van vrijwillige toestemming van betrokkenen wordt gebruikt.

5.2 Kaders apps onduidelijk

Uit de aangeleverde documenten blijkt dat er kaders ontbreken over de verantwoordelijkheden in het proces nu, en in een situatie waarin de apps in gebruik zouden zijn, terwijl dit voor gebruikers van de app volkomen helder moet zijn. De doelstellingen van de apps zijn niet altijd helder gedefinieerd. Deze dienen

te worden gedefinieerd door de verwerkingsverantwoordelijke; dit kan niet louter aan een app-ontwikkelaar worden overgelaten nu hij de beoogde situationele inzet van de apps onvoldoende kent.

Ten aanzien van de aangeleverde documenten geldt dat deze korte analyses van deskundigen bevatten, maar dat een verdere beschouwing van het ministerie van VWS daarover, ontbreekt. Het ministerie heeft voorts geen afweging aangeleverd waarin de noodzaak van bron- en contactopsporingsapps is aangetoond. Denk hierbij aan de afweging van alternatieven en het aantonen van de proportionaliteit. Ook is van belang dat helder wordt gemaakt waarvoor de app wordt ingezet. De sociaal-maatschappelijke gevolgen kunnen immers groot zijn. Het mag niet zo zijn dat wanneer iemand geen gebruik kan of wil maken van een app, toegang tot werk, school of bijvoorbeeld een supermarkt wordt geweigerd. Dit betekent dat het ministerie van VWS helder moet zijn over de kaders waarbinnen de app gebruikt mag worden.
Voor zover de app-voorstellen verder uitgewerkt zijn, stelt de AP vast dat een beoordeling van gegevensbeschermingsrechtelijke aspecten in deze fase van het proces moeilijk is. De reden hiervoor is dat fundamentele keuzes - een juridisch raamwerk - over onder andere de verwerkingsverantwoordelijkheid, het precieze doel van de verwerking en de grondslag voor de verwerking, nog niet gemaakt zijn. Als logisch gevolg daarvan kon daarmee bij het ontwikkelen van de apps geen rekening worden gehouden. Die keuzes zullen naar het oordeel van de AP van grote invloed zijn op de inrichting van de te ontwikkelen app. Pas als die keuzes zijn gemaakt, kan een beoordeling van de rechtmatigheid van de verwerking van persoonsgegevens met de te ontwikkelen app plaatsvinden, waarbij fundamentele vragen over bijvoorbeeld noodzakelijkheid, doelbinding, dataminimalisatie en de rechten van betrokkenen kunnen worden beantwoord.

5.3 Doelen onscherp geformuleerd

Het doel van de verwerking van persoonsgegevens die de app meebrengt, in sommige gevallen meerdere doelen, zijn kritisch bekeken met het oog op de eis van doelbinding. Dat is een van de principes van de AVG. Het feit dat sommige apps meerdere doelen nastreven ziet de AP als een risico voor de gegevensbescherming. De beoordeling van de vraag of de verwerking van persoonsgegevens als gevolg van het gebruik van de corona-app noodzakelijk is gelet op de daarmee nagestreefde doeleinden, kon door de AP niet worden gemaakt. Enerzijds omdat de doeleinden nog niet scherp zijn geformuleerd en anderzijds omdat geen van de voorstellen informatie bevatte over de (bewezen) effectiviteit van de contact tracing app of een afweging van alternatieven.

5.4 Juridische grondslagen onvoldoende onderbouwd

Het ministerie van VWS heeft een juridische onderbouwing voor de toepassing van een corona-app in Nederland aan de AP verstrekt. Die onderbouwing is weergegeven in twee documenten: de notitie ‘Uitwerking grondslag en juridische inbedding apps VWS/WJZ/ Landsadvocaat 17 april 2020’ en het ‘Aanbouwdocument juridische verantwoording corona-apps van de landsadvocaat van 18 april 2020’.
Deze documenten bieden naar de mening van de AP zinvolle aanknopingspunten voor een nadere doordenking van de juridische aspecten en mogelijkheden van de inzet van apps voor bron- en contactopsporing ter bestrijding van het coronavirus.
Tegelijk maakt de AP uit alle ter beschikking gestelde documenten op dat er op het moment van beoordeling tussen het ministerie en de geselecteerde app-ontwikkelaars geen eenduidig beeld lijkt te bestaan van hoe de grondslagen invulling zouden moeten krijgen.

5.5 Welke gegevens zijn minimaal nodig?

De AP constateert dat de verschillende app-ontwikkelaars veel documentatie binnen korte tijd hebben kunnen aanleveren en dat dit een aanzienlijke inspanning heeft gekost bij de app-ontwikkelaars. De AP

constateert dat app-ontwikkelaars soms aannames hebben moeten doen omdat nog niet alle uitgangspunten rondom de app duidelijk zijn geformuleerd. Deze aannames zorgen ervoor dat een beoordeling complex wordt omdat er daarmee geen zekerheid is over de vraag of de aannames van de app-ontwikkelaars overeenstemmen met de uitgangspunten zoals deze later ook door VWS worden gedefinieerd. De vraag welke gegevens noodzakelijk zijn, valt tegen deze achtergrond eveneens niet goed te beantwoorden. Een beoordeling van het beginsel van dataminimalisatie uit de AVG was daarom niet mogelijk.

5.6 AVG rechten onvoldoende gewaarborgd

Het is voor burgers cruciaal dat voldoende helder is bij wie zij kunnen aankloppen met vragen over de verwerking van hun persoonsgegevens. Omdat op dit moment onduidelijk is wie de verwerkingsverantwoordelijke zal zijn en wie de verwerker, is niet helder wie nu let op de AVG-rechten van burger en daar verantwoordelijkheid voor neemt. Noch de app-ontwikkelaars noch het ministerie kon hier uitsluitsel over geven.

6. Technische bevindingen

6.1 Ten aanzien van de voorgelegde apps

De kwaliteit van de door de verschillende app-ontwikkelaars aangeleverde stukken was sterk wisselend, sommige voorgestelde apps waren in een veel verder gevorderd stadium dan andere voorstellen. Dat wil niet altijd zeggen dat de onderliggende uitgangspunten van de betreffende app incorrect waren. Vanuit het perspectief van de AP kan in het algemeen kan gesteld worden dat de apps ten behoeve van contact tracing die gebruik maken van een decentrale oplossing zonder het gebruik van (aanvullende) persoonsgegevens de grootste potentie hebben om een bijdrage te kunnen leveren aan het ondersteunen van de GGD bij het uitvoeren van contactonderzoek. De door verschillende partijen genoemde onderliggende privacy-vriendelijke oplossingen zijn op dit moment nog niet uitontwikkeld en dat maakt mede dat vragen over de daadwerkelijke werking in de praktijk nog beantwoord moeten worden.

6.2 Focus niet alleen op de front-end maar ook de back-end

De AP heeft in haar technische beoordeling gebruik gemaakt van de door de app-ontwikkelaars aangeleverde documentatie. Deze documentatie was voor een goede beoordeling op technisch vlak niet voldoende. De aangeleverde documenten zagen bijvoorbeeld alleen op een front-end, zonder de back-end in ogenschouw te nemen. Een dergelijke back-end kan een zwakke schakel vormen in de keten, het is bijvoorbeeld van groot belang dat een eventuele terugkoppeling van registraties met het coronavirus ‘besmette’ identificatienummers samen met de overige communicatie goed beveiligd is.

6.3 Ten aanzien van het gebruiken van contact tracing apps

Het is niet aan de AP om te oordelen of een app een effectieve oplossing is voor het ondersteunen van de GGD bij het uitvoeren van contactonderzoek of het voorzien van informatie met betrekking tot de pandemie. Mogelijk zijn hier nader door het ministerie te onderzoeken alternatieven voor. Het is wel nodig om helder te maken wat de afweging is voor de inzet van bepaalde technologieën; in hoeverre is de inzet van een contact tracing app die mogelijk een inbreuk maakt op de persoonlijke levenssfeer van de gebruiker de oplossing? Is er een andere oplossing denkbaar die minder inbreuk maakt op de persoonlijke levenssfeer? Het inzetten van een app kent immers tal van nadelen en onzekerheden, die niet technisch weggenomen kunnen worden.

De aan de AP voorgelegde apps zagen voornamelijk op het bijhouden van interpersoonlijk contact. Op basis hiervan ziet zij twee problemen terugkomen: het gebruik van (herleidbare) identificatienummers en tevens een mogelijke overschatting van de betrouwbaarheid van bluetooth.

6.4 Gebruik van unieke identificatienummers

De AP constateert dat de app-ontwikkelaars over het algemeen kiezen voor de uitwisseling van unieke identificatienummers om bij te houden wie met wie in contact is geweest. Deze unieke identificatienummers kunnen persoonsgegevens zijn waardoor de AVG van toepassing is. Bij een aantal van de gekozen oplossingen zijn deze identificatienummers gemakkelijk te herleiden tot de individuele gebruiker van de apps. Maatregelen tegen de-anomisering ontbreken.

6.5 Vragen over de effectieve inzet van bluetooth-technologie

De voorgelegde apps wisselen de unieke identificatienummers veelal uit door middel van het bluetooth-protocol. Bluetooth kan ingezet worden voor contact-tracing. In de ingediende voorstellen kwam echter niet duidelijk naar voren hoe betrouwbaar het gebruik van bluetooth is, en hoe eventuele tekortkoming zijn op te vangen. Zo is de door de overheid gebruikte richtlijn van anderhalve meter afstand vele malen kleiner dan het gemiddelde bereik van bluetooth. Daarnaast is het bereik afhankelijk van allerlei externe factoren (bijvoorbeeld de signaalsterkte van verschillende apparatuur en de aanwezigheid van fysieke objecten tussen gebruikers).[7] Het is lastig om vervolgens op basis van bijvoorbeeld signaalsterkte in combinatie met contactduur te kunnen bepalen in hoeverre verschillende app-gebruikers met elkaar in contact zijn geweest en wat de kans is dat het coronavirus op die manier verspreid is. Mogelijk kunnen deze nadelen worden gemitigeerd, of zijn de resulterende valse positieven geen belemmering in de praktijk. Een onderbouwing daarvoor, eventueel op basis van simulaties, ontbreekt

[7] Voor meer informatie over het bereik van Bluetooth in verschillende omstandigheden zie https://www.bluetooth.com/learn-about-bluetooth/bluetooth-technology/range/#estimator

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.

AUTORITEIT
PERSOONSGEGEVENS

Contactgegevens

Bezoekadres
(alleen volgens afspraak)
Prins Clauslaan 60
2595 AJ DEN HAAG

Let op: bij bezoek aan de Autoriteit Persoonsgegevens moet u een geldig identiteitsbewijs laten zien.

Postadres
Postbus 93374
2509 AJ DEN HAAG

Telefonisch spreekuur
Op onze website autoriteitpersoonsgegevens.nl vindt u informatie en antwoorden op vragen over de bescherming van persoonsgegevens. Heeft u op deze website geen antwoord op uw vraag gevonden? Dan kunt u contact opnemen met de publieksvoorlichters van de Autoriteit Persoonsgegevens tijdens het telefonisch spreekuur via telefoonnummer **0900-2001 201**. De publieksvoorlichters zijn bereikbaar op werkdagen van 09.30 tot 12.30 uur. (5 cent per minuut, plus de kosten voor het gebruik van uw mobiele of vaste telefoon).

Persvoorlichting
Journalisten en redacteuren kunnen met vragen terecht bij de woordvoerders van de Autoriteit Persoonsgegevens. Zie de contactgegevens van de woordvoerders van de AP op deze pagina.

Zakelijke relaties
Bent u een zakelijke relatie van de Autoriteit Persoonsgegevens, zoals een leverancier, dan kunt u ons telefonisch bereiken via telefoonnummer **070-8888 500**.