Uitwerking grondslag en juridische inbedding apps VWS/WJZ/Landsadvocaat 17 april 2020.

Deze notitie ziet op twee apps:[1]
a. de Contact app waarmee de bron-en contactopsporing kan worden ondersteund.

b. de medische hulp app, waarmee een betrokkene die o.g.v. de Contact app een alert heeft gehad dat hij in de nabijheid is geweest van iemand die positief getest is op COvid-19 vervolgens contact op kan nemen met de GGD om te vragen wat hij het beste kan doen.

Uitgangspunt: De inzet en het beheer van de app vindt plaats op grond van de Wet publieke gezondheid
De Wet publieke gezondheid (Wpg) biedt reeds een afdoende basis voor het gebruik van de app. Het doel van de app is immers de GGD te ondersteunen bij het bron- en contactonderzoek, dat bij het stapsgewijs loslaten van de huidige beperkingen een belangrijke rol gaat spelen. Als gezegd, staat de Wpg het (door de GGD) laten uitvoeren van bron- en contactonderzoek reeds toe. De wijze waarop dit plaatsvindt is in beginsel vormvrij, hetgeen ruimte biedt om als ondersteunende tool bij het verrichten van bron- en contactonderzoek een app aan te bieden die burgers vrijwillig kunnen gebruiken. De minister wijst meer concreet op de volgende wettelijke grondslagen:

- Artikel 9, tweede lid, aanhef en onder h, AVG jo. artikel 6, eerste lid, aanhef en onder e, AVG bepaalt dat de verwerking van bijzondere gegevens (in dit geval gezondheidsgegevens) is toegestaan indien de verwerking noodzakelijk is om redenen van algemeen belang op het gebied van volksgezondheid ter uitvoering van een publieke wettelijke taak. Voorwaarde daarbij is dat de verwerking is uitgewerkt in een Unierechtelijke of lidstatelijke bepaling waarin passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van anderen (met name het beroepsgeheim). De Wpg bevat, zoals hieronder zal worden toegelicht, dergelijke wettelijke grondslagen ter bescherming van zwaarwegende algemene belangen van volksgezondheid.
- De minister (van VWS) heeft op grond van artikel 3, eerste lid, Wpg de taak om de kwaliteit en de doelmatigheid van publieke gezondheidszorg te bevorderen. In aanvulling draagt hij zorg voor de instandhouding en de verbetering van de ondersteuningsstructuur. De minister heeft bovendien op grond van artikel 7, eerste lid, Wpg de leiding bij de bestrijding van een infectieziekte uit groep A, zoals het Coronavirus.
- Een arts is op grond van artikel 22, eerste lid, Wpg verplicht om bij de GGD een melding (bestaande uit onder meer naam, BSN, ziektebeeld en eerste ziektedag) te doen van een vastgestelde besmetting.
- De GGD is op grond van artikel 29 Wpg verplicht om een dergelijke melding te registreren;
- De GGD moet die melding bovendien doorsturen naar het RIVM (Artikel 28 Wpg; niet op naam, wel met vermelding eerste drie cijfers postcode van patiënt);
- De GGD heeft vervolgens de wettelijke taak om bron- en contactopsporing te verrichten (artikel 6, eerste lid, aanhef en onder c, Wpg). Het uitvoeren van een dergelijk bron- en contactopsporing vindt altijd plaats op grond van de vrijwillige medewerking van de besmette betrokkene (*Kamerstukken II* 2007/08, 31 316, nr. 3, p. 35-36). De app betreft een ondersteunende tool voor het verrichten van het contactonderzoek. Een deel van het verrichten van het contactonderzoek wordt geautomatiseerd in de zin dat een gebruiker zelfstandig met zijn smartphones (via een backend server) kan vaststellen of hij mogelijk een risico op besmetting heeft gelopen. De Wpg biedt reeds nu al de benodigde ruimte om een dergelijke app voor contactonderzoek in te zetten. Artikel 6, eerste lid, aanhef en onder c, Wpg laat de precieze wijze waarop het contactonderzoek wordt verricht door de GGD immers open.
- Het beheer van de app door de GGD leidt tot een optimale bescherming van de privacy van de betrokkene. De GGD verkrijgt in beginsel géén inzage in persoonsgegevens. Ook voor zover dat anders zou zijn (bijvoorbeeld omdat de backend-server gepseudonimiseerde gegevens bevat), merkt de minister op dat de GGD géén inzage verkrijgt in andere gegevens dan waarover zij reeds in het kader van een contactonderzoek zou mogen beschikken. Tot slot is de GGD bij constatering van een (mogelijke) besmetting een behandelrelatie mogelijk tussen besmette burger-GGD waarvoor ook een geheimhoudingsplicht is geregeld. Daarmee is voldaan aan de verplichting van artikel 9, tweede lid, aanhef en onder i, AVG dat bepaalt dat bij de verwerking van

[1] Zie pagina 5 e.v. in Kamerbrief van 16 april 2020:
https://www.rijksoverheid.nl/documenten/kamerstukken/2020/04/15/covid-19-update-stand-van-zaken

persoonsgegevens ter bescherming van een zwaarwegend algemeen op het gebied van volksgezondheid het beroepsgeheim geborgd moet zijn.

-
- Het voorgaande maakt dat, voor zover in het kader van de apps al (gepseudonimiseerde) persoonsgegevens worden verwerkt door de GGD, artikel 9, tweede lid, aanhef en onder i, AVG jo. artikel 6, eerste lid, aanhef en onder e, AVG jo. artikel 6, eerste lid, aanhef en onder c, Wpg daarvoor een wettelijke grondslag vormt.
-

Uit het voorgaande volgt dat de Contact app als volgt zal worden ingericht:

1. **Vrijwilligheid voor burgers** in downloaden, opslag apparaat en vrijgeven bij besmetting. Via een communicatietraject burgers oproepen om mee te doen.
2. **Inhoudelijke beheer bij GGD:** de wettelijke taak maakt de GGD tot deskundige en daarmee ook veilige/betrouwbare partij voor de burger en tevens kan de GGD o.g.v. die wettelijke taak gelden als 'Health Authority" in de zin van de draft guidance van de EC. De deskundigheid van de GGD staat ook garant voor de betrouwbaarheid van de gegevens, wat bijv. voor het RIVM van cruciaal belang is.
3. **App's mogen niet verder gaan dan de taak en het doel van de GGD'n vanuit de Wpg**.
4. Met de keus voor de Wpg (de tijdelijke maatregelen in verband met de Coronacrisis) is ook de noodzakelijke **tijdelijkheid** automatisch geregeld: de apps worden ingezet zolang dat nodig is ter bestrijding van de Coronacrisis, niet langer. Dit betekent dat er geen doorontwikkeling mogelijk is voor latere doeleinden.

ID's op telefoon

Uitgangspunt is dat er enkel random gegenereerde ID's worden opgeslagen lokaal op de telefoon van de gebruiker. In deze fase worden er door de GGD nog geen persoonsgegevens verwerkt. Uit het ID is niet af te leiden om welke persoon het gaat. De GGD heeft geen toegang tot de ID's. Evenmin vindt er een gegevensverstrekking plaats met de GGD.

Mocht de app op een manier worden ingericht die maakt dat er sprake is van pseudoniemen (in plaats van anonieme ID's), dan kan het – afhankelijk van de inrichting van de app – mogelijk zijn dat sprake is van de verwerking van persoonsgegevens. Ook hier geldt echter dat de GGD geen toegang heeft tot de gegevens in de app van de gebruiker. De GGD zal echter slechts feitelijk (gepseudonimiseerde) persoonsgegevens verwerken als het ID van de besmette gebruiker naar de backend-server wordt gestuurd en het ID wordt opgeslagen op de backend server (zie hierna). In dat geval verwerkt de GGD als beheerder de ID's op de backend server. Die verwerking van persoonsgegevens kan dan worden gebaseerd op het wettelijk kader van de Wpg, zoals dat hierna beschreven wordt.

Verwerking van persoonsgegevens

Op het moment dat er een melding wordt gedaan van een besmetting aan de GGD en de gebruiker van de app de ID's vrijgeeft, is er sprake van de verwerking van persoonsgegevens. Afhankelijk van de uiteindelijke oplossing zijn er twee opties mogelijk:

1 (na objectieve verificatie van de arts) verzendt de smartphone van de besmette gebruiker zijn sleutel en het overzicht van zijn ID's naar de backend server. De backend server wordt beheerd door de GGD en bevat een overzicht van de ID's waarvan de afgelopen dagen is vastgesteld dat de gebruiker besmet is. De app van de andere gebruikers controleert dagelijks of de gebruiker eventueel in contact is geweest met een besmette gebruiker. De koppeling van de ID van de besmette gebruiker met de ID van andere gebruikers vindt plaats op de telefoon van de andere gebruikers. Ook de risico-analyse vindt plaats op de telefoon van de gebruiker. De rol van de GGD is beperkt tot het beheren van de backend server. De app fungeert als een geautomatiseerd waarschuwingssysteem dat het contactonderzoek van de GGD automatiseert.

2 (na objectieve verificatie van de arts) voert de GGD aan de hand van het overzicht van de ID's op de smartphone van de besmette gebruiker een risicoanalyse uit (bijv. nabijheid en duur contact). De GGD selecteert de ID's die mogelijk risico hebben gelopen. De besmette gebruiker verkrijgt een autorisatie of code om de (door de GGD) geselecteerde ID's geautomatiseerd te waarschuwen. Dit vindt plaats doordat de gebruiker zijn sleutel en het

overzicht van de geselecteerde ID's naar de backend server stuurt. De backend server wordt beheerd door de GGD en bevat een overzicht van de ID's waarvan de afgelopen dagen is vastgesteld dat de gebruiker besmet is. De app van de andere gebruikers controleert dagelijks of de gebruiker eventueel in contact is geweest met een besmette gebruiker. De koppeling van de ID van de besmette gebruiker met de ID van andere gebruikers vindt plaats op de telefoon van de andere gebruikers.

De GGD heeft in beide gevallen een wettelijke grondslag om persoonsgegevens en bijzondere persoonsgegevens te verwerken in het kader van bron –en contactonderzoek in de Wpg. Zoals hiervoor reeds toegelicht, kan in beide gevallen – voor zover al (gepseudonimiseerde) persoonsgegevens zouden worden verwerkt door de GGD - de wettelijke grondslag voor het verwerken van dergelijke gegevens gevonden worden in artikel 9, tweede lid, aanhef en onder i, AVG jo. artikel 6, eerste lid, aanhef en onder e, AVG jo. artikel 6, eerste lid, aanhef en onder c, Wpg.

De inzet van de app past dus binnen de taak die de GGD uitvoert. De kwalificatie van de app is een belangrijk gegeven. Wij kwalificeren de app dusdanig dat het gaat om ondersteuning van het bron en contactonderzoek. De GGD blijft de enige partij die de wettelijke taak heeft om bron- en contactopsporing te verrichten en verkrijgt daartoe ook de noodzakelijke bijzondere persoonsgegevens. De app is dienstbaar ten behoeve van de taak van de GGD. De GGD heeft een taak als er een besmetting wordt vastgesteld en in het kader van het handelen ten behoeve van die taak is de app in deze fase van de bestrijding in wezen een noodzakelijke ondersteuning. De exit strategie om uit de crisis te komen vergt dat er voor veel meer burgers contact onderzoek gedaan moet worden. De app ondersteunt hierbij en wordt ook alleen maar gebruikt ter ondersteuning van die taak.

Als we binnen dit kader van de Wpg blijven is er naar de mening van VWS/WJZ/Landsadvocaat geen nieuwe of nadere wettelijke regeling nodig.[2]

Rol van de medische hulp app
Voorstel is dat het alert dat via de Contact app wordt gezonden na een besmetting een link bevat met informatie en het advies contact op te nemen met huisarts of GGD. Iemand kan dit dan vrijwillig doen. De eventuele ondersteuning met de medische hulp app in het verdere contact kan dan alleen ter ondersteuning van de reguliere behandelrelatie zijn die dan ontstaat tussen (mogelijk) besmette burger-GGD. Het beheer/inzet van die app ligt dan óók bij de GGD. Hier mag geen derde partij tussen zitten. Tevens is relevant dat er op grond van de Wpg een geheimhoudingsplicht geldt. Tevens is belangrijk dat de Contact app en deze medische hulp app complementair zijn.

[2] Over de vormgeving van de constructie: Eigendom of licentie, beheer beleggen bij de GGD'n en het beleggen van het technische beheer is separaat advies van de landsadvocaat gevraagd.