VWS brief in reactie op brief NCTV dd. 16-4-2020 met kenmerk 2889657

Geachte (10)(2e) (10)(2e),

Ik heb uw brief van 16 april met aandacht gelezen. U beschrijft uw zorgen over risico's voor nationale veiligheid bij de ontwikkeling en inzet van apps voor ondersteuning van bron- en contactonderzoek COVID-19. Ik deel deze zorgen met u, en hecht ook aan een app die veilig is. In het proces dat ik de afgelopen week heb doorlopen is ook een aantal harde randvoorwaarden opgesteld, waarbij ook uitdrukkelijke aandacht is voor veiligheid. Deze randvoorwaarden heb ik vanavond nogmaals herhaald in het debat dat ik met de Tweede Kamer voerde.

In uw brief geeft u een aantal aanbevelingen, die ik hieronder samenvat

- Dataminimalisatie: verwerk data zo kort mogelijk en alleen data die nodig is voor het doel
- Sla gegevens lokaal (decentraal) op en beperk de uitwisseling
- Gebruik niet herleidbare identiteitsgegevens
- Gebruik een veilige verbinding en sla gegevens veilig op
- Waarborgen voor de integriteit en kwaliteit van de gegevens
- Zorg dat de authenticiteit van de app en (ziek)meldingen kan worden geverifieerd.
- Betrek onafhankelijke autoriteiten t.b.v. toezicht op privacy en testen techniek
- Signaleer en verhelp fouten, kwetsbaarheden en misbruik zo snel mogelijk
- Gebruik geen producten, diensten of aanbieders uit landen met een offensief cyberprogramma gericht tegen Nederlandse belangen.

In de marktconsultatie/uitnodiging van zaterdag 14 april hebben wij uitgangspunten meegegeven, die raken aan bovengenoemde aanbevelingen, maar vanwege de vorm van marktconsultatie en op advies van juristen wat globaler zijn geformuleerd. We kunnen in een consultatie namelijk geen technische invulling voorschrijven. Hieronder ga ik op specifieke punten in:

- *Geen gebruik van locatiegegevens*
  In de uitvraag is daarvoor de volgende tekst opgenomen: "Gegevens die het apparaat verlaten mogen op geen enkele wijze iets zeggen over verplaatsingsgedrag, tijdstip, locatie of sociale netwerk van die persoon"

- *Geen gebruik van persoons- en contactgegevens*
  In de uitvraag is daarvoor de volgende tekst opgenomen: "Gegevens die het apparaat verlaten mogen op geen enkele wijze iets zeggen over verplaatsingsgedrag, tijdstip, locatie of sociale netwerk van die persoon"

- *Decentrale opslag*
  Elke tot nu toe voorgestelde oplossing heeft ook een geringe centrale opslag van data nodig (mensen moeten een bevestigde besmetting kunnen doorgeven en anderen moeten op de hoogte kunnen worden gebracht van contact met een besmet persoon). Centrale opslag van persoonsgegevens is wel uitgesloten.

- *Ontwikkeling van apps door betrouwbare aanbieder*
  We konden vooraf geen aanbieders uitsluiten in een consultatie. Dat kan in de volgende stap wel en zal zeker moeten gebeuren!

- *Onafhankelijke kwaliteitscontrole*
  In de uitvraag is daarvoor de volgende tekst opgenomen: "De opzet, bestaan en werking van de beveiliging van de oplossing wordt gecontroleerd op basis van onafhankelijke audits". Daarbij is ook de gesteld dat de broncode openbaar moet zijn en zal deze ook beoordeeld kunnen (en moeten) worden.

- *Kwaliteit en integriteit gegevens*
  In de uitvraag is daarvoor de volgende tekst opgenomen: "valse positieven moeten zoveel mogelijk beperkt worden door de oplossing" en als voorwaarde "beschrijving van controleerbaarheid van de daadwerkelijk gebruikte oplossing"

Vervolgens is een lijst met harde randvoorwaarden opgesteld, die is afgestemd met onder andere de AIVD, NCTV en NCSC, maar ook andere en externe experts. In deze lijst hebben 10 van de 11 randvoorwaarden een relatie met beveiliging en dus ook met nationale veiligheid:

1) Heridentificatie onmogelijk
   a) Een aanvaller kan er niet achter komen wie COVID-19 heeft
   b) Een aanvaller kan er niet achter komen wie op welke locatie is geweest
   c) Een aanvaller kan er niet achter komen met wie app-gebruiker in contact is geweest
2) Openbare broncode en ontwerp
3) Veilig distributiekanaal voor de applicatie (op je telefoon krijgen) – compatibiliteit met app stores
4) Veilige communicatie met back-end
5) Match ziektemeldingen met recente contacten op eigen telefoon OF volledig anoniem
6) Minimaal is de App in het Nederlands EN Engels beschikbaar / configureerbaar.
7) Geen centrale opslag persoons- of locatiegegevens
8) De oplossing is interoperabel op basis van gangbare en open standaarden
9) De gebruiker kan de applicatie verwijderen en daarmee worden ook de gegevens van de telefoon verwijderd.
10) De leverancier van de applicatie biedt de mogelijkheid om updates uit te voeren.
11) De aanbieder verklaart dat de applicatie voldoet aan geldende wet- en regelgeving (Avg etc.).

Het selectieproces is weliswaar kort, maar dat komt om dat VWS vraagt om bestaande oplossingen. Het selectieproces is onderverdeeld in een eerste, grove selectie op basis van deze harde randvoorwaarden. Vervolgens heeft er op 16 april een diepgaandere selectie plaatsgevonden met teams van experts. In zes van de acht teams voor de expertbeoordeling was een medewerker van AIVD, NCTV of NCSC aanwezig, de rest van de plaatsen zijn bezet door externe security experts die nodig zijn voor het maatschappelijk draagvlak.

Op dit moment zijn 8 oplossingen geselecteerd voor de volgende fase: de publieke beproeving. Daarvoor zullen vrijdag 17 april verschillende testen worden uitgevoerd door KPMG, zoals een pentest en code-onderzoek. Ook de Autoriteit Persoonsgegevens zal een quick scan uitvoeren (van vrijdag 17 april tot en met maandag 20 april). Later zal de AP een volledig Voorafgaand Onderzoek gaan uitvoeren. Uiteraard zullen we de uitkomsten delen met de AIVD, NCTV en NCSC. Er is ook afgesproken dat de AIVD, NCTV en NCSC in de gelegenheid worden gesteld om alle documentatie van die oplossingen te reviewen. Daarnaast staan wij open voor verdere suggesties als het gaat om aanvullend onderzoek.

Na dit weekend zullen we de opbrengst bespreken in de MCCB en in de Tweede Kamer; we hebben de Tweede Kamer in het debat vandaag toegezegd geen onomkeerbare stappen te maken.

De volgende stap is de verwerving. Daarin kunnen we, in tegenstelling tot deze marktconsulatie, specifieke eisen stellen, en daar zullen we de AIVD, NCTV en NCSC uiteraard ook bij betrekken. Ik benadruk nogmaals dat er op verschillende momenten in het komende proces de mogelijkheid bestaat om advies te geven op risico's en (mogelijke) maatregelen, randvoorwaarden en aanbevelingen om deze risico's te beperken. Daarmee hoop ik van harte dat ik de komende periode een beroep kan blijven doen op de AIVD, NCTV en NCSC.