Ministerie van Ministerie van Volksgezondheid, Welzijn en Sport

Oproep corona digitale toepassingen

Inleiding

>>>tekst invoegen svp

Doelstellingen
Bij infectieziektecrises is het nodig om tijdig en adequaat bestrijdingsmaatregelen te treffen. De burgemeesters, en in bijzondere gevallen de minister en de voorzitters van de Veiligheidsregio, zijn hiervoor verantwoordelijk. Zonder deskundige inhoudelijke adviezen kunnen zij echter geen goede beleidsbeslissingen nemen. Bij een dreigende crisis kan de directeur van het Centrum Infectieziektenbestrijding van het RIVM daarom een Outbreak Management Team (OMT) bijeenroepen. De opdracht van een OMT is het 'best mogelijke professionele advies' op te stellen voor de verantwoordelijke bestuurders. In het kader van de bestrijding van COVID-19 is dit de afgelopen periode frequent gebeurd.

Het Outbreak Management Team (OMT) adviseerde op 6 april 2020 om z.s.m. de mogelijkheden voor ondersteuning van bron- en contactopsporing m.b.v. mobiele applicaties te onderzoeken om belasting van de GGD te reduceren. Dit deed zij in het kader van de afschalingsstrategie en het bestrijdingsbeleid voor de volgende fase. Het OMT heeft een voorkeur voor een populatiegebaseerde aanpak gebruikmakend van technieken die de privacy van eindgebruikers waarborgen conform de AVG-wetgeving (zie bijvoorbeeld het recente PEPP-PT-initiatief).
Naast dit advies van het OMT zien wij ook initiatieven in regio's gericht op het op afstand begeleiden van mensen met klachten in zelfisolatie teneinde de belasting van de zorg te verkleinen en daarbij er tegelijkertijd voor te zorgen dat op basis van zelfmonitoring kan worden geconstateerd dat intensievere zorg nodig is.

Het doel van deze oproep is om voorstellen te krijgen voor:

- Digitale hulpmiddelen zoals bijvoorbeeld apps die kunnen bijdragen aan bron- en contactopsporing, waarbij stringente eisen worden gesteld aan onder meer snelle beschikbaarheid, privacy en informatiebeveiliging
- Digitale hulpmiddelen zoals bijvoorbeeld apps die kunnen bijdragen aan zelfmonitoring en begeleiding op afstand, waarbij stringente eisen worden gesteld aan onder meer snelle beschikbaarheid, privacy en informatiebeveiliging
- Overige digitale hulpmiddelen zoals bijvoorbeeld apps die kunnen bijdragen aan de afschalingsstrategie en het bestrijdingsbeleid
- De technische en organisatorische wijze waarop privacy en informatieveiligheid het beste geborgd kunnen worden en waarop het beste voldaan kan worden aan de verdere uitgangspunten zoals opgenomen in deze oproep

Procedure
In de eerste ronde wordt de markt gevraagd om schriftelijk antwoord te geven op de bijgevoegde vragen (zie Bijlage 1 bij deze oproep). Op basis van de gegeven antwoorden wordt bepaald of er eventueel in een tweede ronde marktpartijen worden uitgenodigd om de (on)mogelijkheden nader te bespreken en een demonstratie te bekijken.

Dien uw schriftelijke reactie in via dit emailadres:

(10)(2e) @minvws.nl of ZonMW

Planning
De planning van deze oproep is als volgt:

- publicatie vragen aan de markt: 11 april 2020;
- ontvangen antwoorden op de gestelde vragen: uiterlijk 14 april 2020, 12.00 uur;
- bestuderen antwoorden: 14 tot 16 april 2020;
- indien gekozen wordt voor een tweede ronde:
  - uitnodigen marktpartijen: 16 april 2020
  - Hackaton met als doel verbeteren voorstellen en verschaffen van transparantie: 18 en 19 april

Als u na 17 april niets vanuit VWS heeft vernomen, dan sluit uw oplossing onvoldoende aan bij de korte termijn behoeften.

Beschrijving behoefte

VWS ontvangt graag voorstellen van partijen die kunnen voorzien in een slimme digitale oplossing voor:

a) Bron- en contactopsporing, in aanvulling op reguliere bron- en contactopsporing door GGD'en.

b) Het ondersteunen van zelfmonitoring en begeleiding op afstand.

c) Overige aspecten van de afschalingsstrategie en het bestrijdingsbeleid

d) Het op een technische en organisatorische wijze borgen van de privacy en informatieveiligheid en van de verdere uitgangspunten in deze oproep.

Uitgangspunten voor de oplossing

De gelegenheidscoalitie "Veilig tegen Corona" heeft opgeroepen om aan eisen te voldoen ten aanzien van onder meer privacy en computerbeveiliging. Deze zijn betrokken bij de uitgangspunten die worden gesteld aan de oplossing.

Bron en contactopsporing

- Gegevens zijn niet tot individuen herleidbaar.
- Het moet onmogelijk zijn om met de gegevens, die door de app worden verzameld, gebruikers te deanonimiseren, ook niet als de gegevens worden gecombineerd met andere gegevens. Dit betekent dat het systeem niet gebouwd kan zijn op het gebruik van identificatienummers van hardware of andere identificerende gegevens, zoals het "Bluetooth Device Address".
- De functionaliteit slaat zo min en zo kort mogelijk gegevens op (max 14 dagen tot een maand afhankelijk doel van de app) of verwijdering zodra iemand negatief getest is.
- Dat betekent bijvoorbeeld dat de app geen gegevens over iemands locatie vastlegt, maar slechts het identificerende nummer van andere gebruikers in de buurt. Ook is het niet nodig om het precieze tijdstip van zo'n ontmoeting te registreren. Om de gegevens op tijd te kunnen verwijderen is alleen een datum van registratie nodig, geen locatie.
- valse positieven moeten zoveel mogelijk beperkt worden door afstandmeting in de functionaliteit
- Geen centraal opgeslagen persoonsgegevens.

  Alle gegevens en processen worden in beginsel lokaal op iemands telefoon verwerkt. Dat betekent bijvoorbeeld dat het proces van de beoordeling of een gebruiker recent in contact is geweest met een besmet persoon, bij de gebruiker plaats moet vinden. Mocht het toch nodig zijn om gegevens te delen, bijvoorbeeld na het constateren van een besmetting, dan alleen na vrijwillige, expliciete en geïnformeerde toestemming van de gebruiker. De gegevens die wél de telefoon van de gebruiker verlaten, mogen op geen enkele wijze herleidbaar zijn tot die gebruiker.

Uitgangspunten voor alle voorgestelde functionaliteiten

- Functionaliteiten voldoen aan gangbare beveiligingsstandaarden voor:
  - Vercijferde opslag van lokale data
  - Vercijferde communicatie
  - Code review, gebruikerstest en pentest (de app mag het aanvalsprofiel van de smartphone niet vergroten)
  - Geen datalek bij verlies/diefstal van de smartphone
  - Voldoet aan standaarden Informatiebeveiliging in de zorg NEN 7510, NEN 7512 en NEN 7513
- Voldoen aan ISO/IEC 25010 Kwaliteit van Software: proceskwaliteit, systeemkwaliteit, gegevenskwaliteit
- Als er functionaliteiten worden aangeboden moeten deze reeds bestaan, uitontwikkeld zijn en werken in een productie omgeving
- De functionaliteiten moeten binnen enkele dagen breed uitgerold kunnen worden naar burger in Nederland
- Het doel richt zich op slechts één doel; het onder controle krijgen van het virus.
- Het gebruik moet gericht zijn op het vereenvoudigen van contactonderzoek en zelfmonitoring en daarmee het informeren en beschermen van individuen.
- Gebaseerd op wetenschappelijk inzicht en bewezen effectief.
- De inzet van de functionaliteit en de daarmee verzamelde gegevens moet gebaseerd zijn op wetenschappelijke kennis en aantoonbaar bijdragen aan het onder controle krijgen van het virus.
- De functionaliteit moet het mogelijk maken om vooraf te testen op een beperkte groep gebruikers, zodat op basis hiervan beoordeeld kan worden dat deze noodzakelijk, effectief en proportioneel is.
- Signalering via de functionaliteit is gebaseerd op wetenschappelijk bewezen effectiviteit
- De broncode van de applicatie en de overige infrastructuur is openbaar onder een vrije software licentie, zodat iedereen de werking van het systeem kan controleren.
- Beschrijving van controleerbaarheid van de daadwerkelijk gebruikte functionaliteit.
- De inzet van de applicatie is per definitie tijdelijk.
- Als de applicatie niet meer effectief of noodzakelijk is, moet de uitrol kunnen worden teruggedraaid en data kunnen worden verwijderd.
- De functionaliteit moet ook tijdelijk kunnen worden uitgeschakeld.
- Data minimalisatie is uitgangspunt
- Beschreven aantoonbare aandacht voor vertrouwelijkheid en integriteit
- Dat kan door het gebruik van encryptie en andere beveiligingstechnologiën. Uit de verzending van gegevens is al af te leiden dat de desbetreffende gebruiker mogelijk besmet is.
- Gebruiksvriendelijk

Intuïtief in gebruik, duidelijke handleidingen, helder waar hulp kan worden gevonden.
- breed toegankelijk,

Beschrijving van hoe om te gaan met mensen die niet beschikken over bijvoorbeeld een smartphone of speciale aanpassingen behoeven

- de functionaliteit ondersteunt meertaligheid
- De functionaliteit is efficiënt, waaronder zo min mogelijk beslag op batterijcapaciteit
- De functionaliteit dient eenvoudig te kunnen worden geupdate om bijvoorbeeld crashes te verhelpen
- Functionaliteiten kunnen met toestemming van de gebruiker zelf worden geinstalleerd en verwijderd
- De functionaliteit gaat uit van werking op basis van vrijwilligheid burgers

Vragen aan de markt

VWS heeft verschillende vragen. Deze vragen leest u in Bijlage 1 (Vraag- en Antwoordformulier). De vragenlijst is met zorg opgesteld. VWS realiseert zich dat de beantwoording van de vragen de nodige tijdsinspanning vraagt. Deze investering is van belang en van toegevoegde waarde om een opdracht in de markt te zetten die aansluit op de markt.

Stel uw beantwoording bij voorkeur op in de Nederlandse taal. Elk antwoord dient overtuigend, volledig, relevant, eenduidig, onderscheidend te zijn en beschreven in maximaal 2 A4's per vraag, met in totaal maximaal 8 A4's voor alle vragen.