Ministerie van Ministerie van Volksgezondheid, Welzijn en Sport

Bijlage 1 Vraag- en antwoordformulier

Gegevens Uitnodiging	
Titel	Uitnodiging slimme digitale oplossingen Corona
Opdrachtgever	De Staat der Nederlanden (ministerie van Volksgezondheid, Welzijn en Sport)

Gegevens Ondernemer	
Naam Ondernemer	(10)(2e)
Adresgegevens Ondernemer	(10)(2g) , (10)(2g)(10)(2g) (10)(2e)
Contactpersoon Ondernemer	(10)(2e) (10)(2e) (10)(2e)
Functie contactpersoon	Senior Security Specialist
E-mailadres Ondernemer	(10)(2e) @s (10)(2e) .nl
Telefoonnummer Ondernemer	06-4 (10)(2e)
Website Ondernemer	https:// (10)(2e) .nl

Verklaring	
Ondernemer verklaart dat:	*Doorstrepen wat niet van toepassing is*
De aangeboden oplossing voldoet aan de in de uitnodiging geschetste uitgangspunten en is per 28 april 2020 productierijp	Ja ~~/ Nee~~
De aangeboden oplossing is per 18 april 2020 beschikbaar voor een publieke proef.	Ja ~~/ Nee~~

Omwille van een efficiënte werkwijze vragen we u om een compacte beantwoording en/of beschrijving van uw mogelijkheden ten aanzien van de beoogde oplossing. We verzoeken u dringend om informatie die niet direct de kern van de oplossing raakt, niet in het hoofddocument te verwerken maar als bijlage op te nemen.

1	
Doelstelling	Het verkrijgen van een voorstel voor slimme digitale oplossingen zoals bijvoorbeeld apps die kunnen bijdragen aan **bron- en contactopsporing**, waarbij stringente eisen gelden voor onder meer snelle beschikbaarheid, privacy en informatiebeveiliging
Vraag	Welke slimme digitale oplossing kunt u leveren die bij kunnen dragen aan bron- en contactopsporing?
Antwoord	Onze oplossing werkt door (WiFi) gegevens van een smartphone te registreren. Hierbij is geen app nodig. Deze gegevens betreft unieke MAC-adressen welke elke smartphone heeft. Dit unieke gegeven (MAC-adres van smartphone) wordt op vooraf bepaalde openbare plaatsen gedetecteerd via geïnstalleerde sensoren en vervolgens opgeslagen (middels hashing) zodat het niet mogelijk is om de geregistreerde gegevens te herleiden naar een natuurlijk persoon. In een database (benaderbaar via website) worden alle gedetecteerde unieke smartphone kenmerken opgeslagen. Deze kenmerken kunnen geclassificeerd worden als geïnfecteerde. Voorts krijgt de bevolking de mogelijkheid de eigen smartphone in de database op te zoeken om te kijken of er besmetting kan zijn geweest. De contactmomenten met een geïnfecteerde (MAC-adres) worden inzichtelijk gemaakt op de website door bijv. het invoeren van een telefoonnummer. Onze digitale oplossing om de bron en contactopsporing van geïnfecteerde personen te detecteren is bijzonder omdat de gedetecteerde adressen van smartphones niet herleidbaar zijn (door gebruikmaking van hashing). De bron van besmetting wordt wel inzichtelijk gemaakt. Een database (te benaderen voor bevolking via website) verzamelt alle gedetecteerde informatie. Het identificeren van een persoon op basis het unieke adres van de smartphone is uitsluitend mogelijk in de volgende twee scenario's; **1. En persoon besmet met het virus. Diens identiteit is bekend waardoor zijn/haar smartphone in het systeem is/wordt geïdentificeerd.** **2. De mogelijkheid voor anderen om zijn/haar smartphone op te zoeken in het systeem (openbare database op website of app).** Onze oplossing werkt vanuit de gegevensregistratie van een smartphone door gebruik te maken van het unieke MAC-adres dat elke smartphone heeft. Dit unieke gegeven (MAC-adres van smartphone) wordt vervolgens als hash opgeslagen zodat deze niet herleidbaar is naar een natuurlijk persoon. Elke smartphone heeft een uniek MAC-adres. Een MAC-adres is een vrijwel uniek identificatienummer dat aan een apparaat in een ethernetwerk is toegekend. Door te werken met de gegevensregistratie van MAC-adressen van smartphones worden alle smartphones gevolgd doordat op openbare gelegenheden **sensoren** worden geplaatst. **Methode:** **Bron en contactopsporing van geïnfecteerde personen door contactopsporing van MAC-adressen van smartphones en deze vervolgens niet herleidbaar te maken naar een natuurlijk persoon via database (geen app).** - **MAC-adressen opslaan als hash**

- **Gegevensregistratie door WiFi Probes**
- **Identificatie door plaatsen van sensoren**
- **Gebaseerd op privacy en keuzevrijheid**
- **Opslag van gegevens in centrale database**
- **Koppeling aan begeleiding apps eenvoudig mogelijk**
- **Eenvoudige uitrol mogelijk**
    - Uitrol is pragmatisch. Gezien de minimale software en hardware eisen kan de sensor gebruikmaken van een computer, laptop, Raspberry PI, consumenten routers/access points etc.
    - Snelle uitrol mogelijk door deze minimale systeemvereiste en flexibiliteit in hardware

Privacy door hashing
Het unieke kenmerk van de smartphone (MAC-adres) zal als hash worden opgeslagen. Deze hash komt tot stand met een algoritme dat niet terug herleidbaar is naar het MAC-adres van de smartphone. Alleen op basis van een bekend MAC-Adres kan de Hash worden berekend en tot de registratie komen. In onze oplossing wordt er een database aangelegd. Deze database bevat geen gegevens die herleid kunnen worden naar een natuurlijk persoon tenzij deze personen hier zelf, expliciet, toestemming voor geven. Zie '**Wanneer identificatie van personen**'.

Gegevensregistratie door WiFi probes
Bezoekersregistratie op basis van WiFi probes. Alle Smartphones beschikken over WiFi die, (gemiddeld) iedere 2 minuten zichzelf op basis van een unieke sleutel, identificeren.

Identificatie van smartphones door het plaatsen van sensoren.
Op aangewezen entrees van openbare plaatsen sensoren plaatsen.
Daar waar mensen samenkomen (supermarkten, bedrijfsvestigingen, verzorgingstehuizen, personeelsingang in ziekenhuis, sociale ontmoetingsplaatsen met een entree) **sensors** te plaatsen die deze identificatie opvangt.

Sensoren
Hardware en software vereisten voor sensoren is minimaal. Software hiervoor maakt gebruik van bestaande middelen. Complexiteit van oplossing is laag. Digitale communicatie is (sensors met database) eenvoudig en kan middels beveiligde en versleutelde (TLS) communicatie.

Te ontwikkelen voor deze oplossing:
- Web portaal voor rapportage
- Web portaal om smartphones op te zoeken (koppeling naar personen)
- Centrale database
- Sensoren

bron- en contactopsporing
Door gegevensregistratie van de unieke adressen van smartphones kan worden herleid welke andere apparaten in de nabijheid zijn geweest. Immers het unieke gegeven (MAC-adres van smartphone) zal als hash worden opgeslagen zodat deze **niet** herleidbaar is naar een natuurlijk persoon. Naast dit unieke gegeven zal tevens het tijdstip en duur van de registratie worden opgeslagen.

minimale dataopslag
Daarbij betreft deze beperkte hoeveelheid aan informatie het minimale om binnen de kaders van dataminimalisatie, proportionaliteit en subsidiariteit het volgen van personen mogelijk te maken.

Centrale Database
De verzamelde informatie (unieke sleutels van smartphones, locatie van registratie en tijdstip) zal worden opgeslagen in een centrale database. Vanuit deze database is

	rapportage mogelijk om te herleiden welk potentieel contact een besmet persoon heeft gehad. De centrale database, geplaatst op een veilige locatie (datacenter) in Nederland zal rapportage mogelijk maken vanuit verschillende perspectieven. **Wanneer identificatie van personen** Het identificeren van een persoon op basis het unieke adres van de smartphone uitsluitend mogelijk in de volgende twee scenario's; **1. En persoon besmet met het virus. Diens identiteit is bekend waardoor zijn/haar smartphone in het systeem is geïdentificeerd.** **2. De mogelijkheid voor anderen om zijn/haar smartphone op te zoeken in het systeem (openbare database op website of app).** **Keuzevrijheid opsporing website** Geef de database vrij op een website waardoor iedereen met de eigen smartphone kan zoeken in de database. Op de website kan iedereen zelf zijn haar gegevens invoeren om te zoeken of hij/zij in contact zijn geweest met iemand die besmet is met het virus. Deze actie zal de eigen smartphone identificeren in de database. Hierdoor bestaat de mogelijkheid om, na toestemming van de burger, het gegeven herleidbaar te maken naar een natuurlijk persoon. Denk hierbij aan het opvoeren van een telefoonnummer. **Stimulans voor bevolking zoeken op MAC-adres in de openbare database (hetzij via een website website, hetzij via een app)** Dagelijks wordt op de website (en/of in de media per plaats (stadsdeel, dorp of stad of gemeente) bekend gemaakt waar mogelijk besmetting kan hebben plaatsgevonden (getallen). Door Identificatie van het unieke besmette MAC-adres van de smartphone. Na besmetting (positieve test) is de identiteit bekend en kan deze gekoppeld worden aan het unieke kenmerk in de database.

2	
Doelstelling	Het verkrijgen van een voorstel voor slimme digitale oplossingen zoals bijvoorbeeld apps die kunnen bijdragen aan **zelfmonitoring en begeleiding op afstand**, waarbij stringente eisen gelden voor onder meer snelle beschikbaarheid, privacy en informatiebeveiliging
Vraag	Welke slimme digitale oplossing kunt u leveren die bij kunnen dragen aan zelfmonitoring en begeleiding op afstand?
Antwoord	**Zelfmonitoring en begeleiding op afstand door bron- en contactopsporing** Door gegevensregistratie van de unieke adressen van smartphones in een **database (website)** te plaatsen kan worden herleid welke andere apparaten in de nabijheid zijn geweest. Het unieke gegeven (MAC-adres van smartphone) wordt als hash opgeslagen waardoor deze **niet** herleidbaar is naar een natuurlijk persoon maar wel herleidbaar naar een geïnfecteerd MAC-adres. Het **geïnfecteerde (gehashde) MAC-adres is bekend** in de database. Indien een website openbaar wordt gemaakt waar alle unieke kenmerken traceerbaar zijn kan men zelf herleiden of de eigen smartphone in de buurt of in aanraking is geweest met een geïnfecteerd 'kenmerk'. Indien er **bevestigend contact** is geweest met een geïnfecteerd MAC-Adres dan kan via de website (database) een eenvoudige link naar de te downloaden begeleiding app (b.v. LUSCCI) waardoor: 1. Deelname aan app op vrijwillige basis (hier wordt identiteit pas bekend) 2. Men zichzelf kan monitoren op virus klachten

	3. Men krijgt actieve begeleiding bij klachten 4. Begeleiding op afstand doet druk op 1e lijns zorgverlener afnemen 5. Begeleiding op afstand doet besmettingsgevaar voor zorgverlener afnemen 6. Indien klachten toenemen is patiënt reeds kaart gebracht 7. Patiënt in vroegtijdig stadium testen 8. Patiënt en gezin z.s.m. isoleren 9. Patiënt in zo vroeg mogelijk stadium traceren 10. Na positieve test de geïnfecteerde persoon bekendmaken in de database (lees website) zie doelstelling 1. NB. bezoekersregistratie door opslaan gehashde MAC-adres. Vanuit een database rapportage de mogelijkheid bieden om te herleiden waar, wanneer en hoe laat er potentieel contact kan zijn geweest met een geïnfecteerd persoon (lees MAC-adres smartphone). Hierbij zal deze persoon zelf toestemming moeten geven voor het herleidbaar maken naar een persoonsgegeven in kader van **zelfmonitoring en begeleiding op afstand** . Dit kan eenmalig of permanent zijn. Het naar een natuurlijk persoon herleidbaar maken van de geregistreerde gegevens is dus uitsluitend mogelijk met **toestemming van de persoon**. Tegelijk worden alle smartphones (en daarmee personen) geregistreerd zodat er op aantallen en geografische informatie alsnog sturing op strategie kan plaatsvinden.

3	
Doelstelling	Het verkrijgen van voorstellen voor overige digitale oplossingen, zoals bijvoorbeeld apps, die kunnen bijdragen aan **de transitiestrategie en het bestrijdingsbeleid**
Vraag	Welke slimme digitale oplossingen kunt u leveren die bij kunnen dragen aan de afschalingsstrategie en begeleiding op afstand?

Antwoord	Door gegevensregistratie van de unieke adressen van smartphones in een **database (website en/of app)** te plaatsen kan worden herleid welke andere apparaten in de nabijheid zijn geweest. Het unieke gegeven (MAC-adres van smartphone) is als hash opgeslagen waardoor deze **niet** herleidbaar is naar een natuurlijk persoon maar wel herleidbaar naar een geïnfecteerd (bekend) MAC-adres. Het geïnfecteerde MAC-adres is/wordt immers bekend in de database (als hash opgeslagen).
	
	Indien een website openbaar wordt gemaakt waar alle gehashde MAC-adressen traceerbaar zijn kan men zelf onderzoeken of de eigen smartphone in de buurt of in aanraking is geweest met een geïnfecteerd MAC-adres.
	
	• De centrale database (gepubliceerd op website) staat in een beveiligde omgeving (datacentrum in Nederland) en maakt rapportage mogelijk vanuit verschillende perspectieven mogelijk:
	  ○ bron en contactopsporing
	  ○ preventie (dichtheid meten en voorspellingen)
	  ○ gedrag en in welke mate men opvolging geeft aan het beleid
	  ○ mate van bezoek aan website
	  ○ bereidwilligheid tot medewerking
	  ○ awareness
	• Awareness, zelfmonitoring en begeleiding op afstand door mensen zelf in staat te stellen hun smartphone te identificeren (zelfbeschikking)
	• Complexiteit van oplossing is laag.
	• Begeleiding op afstand doet druk op 1e lijns dienstverlener afnemen
	• Begeleiding op afstand doet besmettingsgevaar voor zorgverlener afnemen
	• Snel testen na contact met geïnfecteerd MAC-adres

	• Snel isoleren na contact van persoon en gezin • Eventueel na testen op volledig herstel • Mutatie virus wordt ook in kaart gebracht bij eventueel 2e infectie • Immuniteit wordt ook in kaart gebracht Het naar een natuurlijk persoon herleidbaar maken van de geregistreerde gegevens is dus uitsluitend mogelijk met toestemming van de persoon. Tegelijk worden alle smartphones geregistreerd zodat er op aantallen en geografische informatie alsnog sturing op strategie kan plaatsvinden. In kader van preventie kan op strategische locaties controle worden uitgevoerd. Denk hierbij aan speciale sensoren in een verzorgingstehuizen (kwetsbare groepen). Hier kan, op basis van bezoekers bij de entree, direct worden bepaald of deze zich in de nabijheid hebben begeven van een drager van het virus.

4	
Doelstelling	Het verkrijgen van voorstellen voor **voorwaarden waaronder digitale oplossingen kunnen worden ingezet** (met betrekking tot techniek, inhoud, werking, implementatie, de privacy en informatieveiligheid)
Vraag	Welke voorstellen voor het op technische en organisatorische wijze borgen van privacy en informatieveiligheid kunt u doen?

Antwoord	Werken vanuit de gegevensregistratie van een smartphone door gebruik te maken van het unieke MAC-adres van smartphone. Anonimiteit door het opslaan van het MAC-adres in de vorm van een hash. Door de hashtechniek is het unieke MAC nummer niet herleidbaar is naar een natuurlijk persoon, maar wordt de aanwezigheid in publieke area en of contacten met geïnfecteerde zichtbaar.
	
	Onze oplossing voorziet in de uitgangspunten en heeft als toegevoegde waarde bovenop eisen.
	
	De rol van Secured by Design in deze oplossing omvat het ontwerp, begeleiding, advies en deel de implementatie. Secured by Design beschikt over brede kennis omtrent het security domein en de technologie gebruikt in deze oplossing. Gezien de korte doorlooptijd en omvang van de uitrol is het noodzakelijk om andere partijen hierin mee te nemen en aan te sturen.
	
	• **Alle smartphones worden gevolgd** waarbij de geregistreerde informatie niet herleidbaar is naar een natuurlijk persoon
	• Geen actie vanuit burgers is vereist om deze oplossing mogelijk te maken. Geen afhankelijkheid van motivatie, techniek of kennis (geen software/app op smartphone)
	• Geen app of software op smartphone. Dus ook geen privacygevoelige informatie om af te schermen. Geen systeemvereisten. Burger hoeft niets te doen
	• Fijnmazigheid op basis van het aantal sensoren. Bijvoorbeeld alle KvK geregistreerd op alle vestigingen
	• De centrale database, geplaatst op een veilige locatie (datacenter) in Nederland maakt rapportage mogelijk vanuit verschillende perspectieven
	• De Centrale database (website of app) maakt rapportage mogelijk vanuit verschillende perspectieven:
	  ○ bron en contactopsporing
	  ○ preventie (dichtheid meten en voorspellingen)
	  ○ gedrag en in welke mate men opvolging geeft aan het beleid
	• Awareness, zelfmonitoring en begeleiding op afstand door mensen, de bevolking zelf in staat te stellen hun smartphone te identificeren

	• Oplossing is niet gebonden aan geografische beperkingen. Ook binnen andere EU-Lidstaten inzetbaar
	• Data Minimalisering met proportionaliteit en subsidiariteit centraal. Uitsluitend de minimale hoeveelheid aan informatie t.b.v. het volgen zal worden gebruikt
	• Op basis van bestaande, proven technology, technologieën. WiFi, database, webapplicatie voor rapportage, webapplicatie voor registratie smartphone
	• Hardwarevereisten voor sensoren is minimaal. Software hiervoor maakt gebruik van bestaande middelen.
	  ○ Uitrol kan op basis van pragmatische wijze. Gezien de minimale software en hardware eisen kan de sensor gebruikmaken van een laptop, Raspberry Pi, consumenten routers/access points etc.
	  ○ Snelle uitrol mogelijk door deze minimale systeemvereiste en flexibiliteit in hardware.
	
	<u>Hardwarevereisten</u>
	• Voor sensoren is minimaal. Software hiervoor maakt gebruik van bestaande middelen
	• Complexiteit van oplossing is laag. Digitale communicatie is (sensors met database) is eenvoudig en kan middels beveiligde en versleutelde (TLS) communicatie
	• Te ontwikkelen voor deze oplossing:
	  ○ Web portaal voor rapportage
	  ○ Web portaal om smartphones op te zoeken (koppeling naar personen)
	  ○ Centrale database
	  ○ Sensoren