



Ministerie  
van Ministerie van Volksgezondheid, Welzijn en Sport

## Bijlage 1 Vraag- en antwoordformulier

| Gegevens Uitnodiging |                                                                             |
|----------------------|-----------------------------------------------------------------------------|
| <b>Titel</b>         | Uitnodiging slimme digitale oplossingen Corona                              |
| <b>Opdrachtgever</b> | De Staat der Nederlanden (ministerie van Volksgezondheid, Welzijn en Sport) |

| Gegevens Ondernemer              |                                                                                                     |
|----------------------------------|-----------------------------------------------------------------------------------------------------|
| <b>Naam Ondernemer</b>           | PricewaterhouseCoopers Advisory N.V.                                                                |
| <b>Adresgegevens Ondernemer</b>  | Thomas R Malthusstraat 5 Amsterdam, 1066 JR Netherlands                                             |
| <b>Contactpersoon Ondernemer</b> | 5.1.2e 5.1.2e                                                                                       |
| <b>Functie contactpersoon</b>    | Partner en accountverantwoordelijke Ministerie van VWS                                              |
| <b>E-mailadres Ondernemer</b>    | 5.1.2e @pwc.com                                                                                     |
| <b>Telefoonnummer Ondernemer</b> | + 5.1.2e                                                                                            |
| <b>Website Ondernemer</b>        | <a href="https://www.pwc.nl/nl/themas/covid-19.html">https://www.pwc.nl/nl/themas/covid-19.html</a> |

| Verklaring                                                                                                                      |                                               |
|---------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| <b>Ondernemer verklaart dat:</b>                                                                                                | <i>Doorstrepen wat niet van toepassing is</i> |
| <b>De aangeboden oplossing voldoet aan de in de uitnodiging geschetste uitgangspunten en is per 28 april 2020 productierijp</b> | Ja / Nee                                      |
| <b>De aangeboden oplossing is per 18 april 2020 beschikbaar voor een publieke proef.</b>                                        | 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 <b>bron- en contactopsporing</b> , 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     | N.v.t.                                                                                                                                                                                                                                                        |

| 2            |                                                                                                                                                                                                                                                                              |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Doelstelling | Het verkrijgen van een voorstel voor slimme digitale oplossingen zoals bijvoorbeeld apps die kunnen bijdragen aan <b>zelfmonitoring en begeleiding op afstand</b> , 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     | N.v.t.                                                                                                                                                                                                                                                                       |

| 3            |                                                                                                                                                                            |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Doelstelling | Het verkrijgen van voorstellen voor overige digitale oplossingen, zoals bijvoorbeeld apps, die kunnen bijdragen aan <b>de transitiestrategie en het bestrijdingsbeleid</b> |
| Vraag        | Welke slimme digitale oplossingen kunt u leveren die bij kunnen dragen aan de afschalingsstrategie en begeleiding op afstand?                                              |
| Antwoord     | N.v.t.                                                                                                                                                                     |

| 4            |                                                                                                                                                                                                                            |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Doelstelling | Het verkrijgen van voorstellen voor <b>voorwaarden waaronder digitale oplossingen kunnen worden ingezet</b> (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     | <b>Zie volgende pagina's.</b> Wij melden ons aan om als onafhankelijke partij een rol te spelen om de voorwaarden te kunnen scheppen voor een betrouwbare uitrol en afbouw van de slimme en digitale oplossingen 'Corona'. |

### 1. PwC als uw onafhankelijke partner voor digitale houvast in onzekere tijden

Als er één moment is dat vertrouwen in elkaar belangrijk is, dan is het in de gezamenlijke bestrijding van het Corona virus. Ons doel is "bouwen van vertrouwen" en "oplossen van belangrijke problemen". Wij zouden trots zijn om als de cybersecurity consulting leider wereldwijd en in Europa (Forrester Wave 2019) u te ondersteunen. Wij verbinden ons merk, passie en kunde aan het beschermen van het maatschappelijk belang van deze digitale oplossing: veilig, vrijwillig, tijdelijk en onder regie van onafhankelijke deskundigen.

Wij staan naast u als onafhankelijke en kritische partij die continu en risico-gebaseerd inzicht geeft in mogelijke kwetsbaarheden in de oplossing en u ontzorgt met praktische aanbevelingen. Hiermee zorgen we samen dat de belasting op onze zorginstellingen en GGD's wordt gereduceerd. We bouwen door op onze ervaring met u in eerdere crisis situaties zoals in het PGB dossier en onze samenwerking om continuïteit van het Maasziekenhuis Pantein te borgen.

In sectie 2 delen we onze visie op bestaande initiatieven voor Covid-19 digitale oplossingen, waar wij in secties 3, 4 en 5 uitwerken hoe we u ondersteunen bij procesmatige, technische en juridische borging. Richting uitrol per 28 april ondersteunen we u om de volgende stappen te nemen:

- Samenwerkingsafspraken maken tussen u, de digitale leveranciers en PwC.
- Uitvoeren belangrijkste analyses: zoals een architectuur- en code review, penetratietest en een analyse ten aanzien van minimum standaarden informatieveiligheid en privacy.
- Dagelijks overleg om de belangrijkste bevindingen, adviezen en acties te bespreken.
- Plan opstellen richting uiteindelijke uitfasering van de oplossing en verwijdering data.

Voor een aantal van onze referenties, meer informatie over PwC en ons team zie Bijlagen 2, 3 en 4.

### 2. Onze visie op de route naar productie voor de gevraagde digitale oplossingen

Decentrale oplossingen voor contactonderzoek (zoals DP-3T voorstelt), genieten de voorkeur vanuit privacy oogpunt en schaalbaarheid. In het ontwerp is databescherming geborgd en zijn mogelijkheden tot uitbreidingen van de verwerking technisch geminimaliseerd met controle in handen van de gebruiker. Deze ontwerpen zijn conceptueel incompleet en gezien de tijdsdruk liggen concessies tijdens implementaties op de loer. Voorgestelde toepassingen zijn enkel effectief en veilig als de gehele levenscyclus van de applicatie en data zijn meegewogen. Het ontwerp moet voorzien in maatregelen en updates na livegang. Zoals monitoring op de beoogde differential privacy en het vergelijken van tellingen in de dataset met die van de testcentra en de borging van rechten van betrokkenen. De beveiliging van de gehele keten moet volgens ons aan dezelfde hoge databescherming standaarden voldoen, waarbij bestaande componenten en de te ontwikkelen applicaties in samenhang worden beschouwd. Transparante open-source ontwikkeling zorgt ervoor dat experts uit de diverse disciplines actief kunnen bijdragen.

Het vaststellen van true-positives vraagt om accounts die op de beperkte backend draaien waar asymmetrische cryptografie een rol speelt met bijbehorende logging en monitoring zodat enkel BIG-geregistreerden deze functie kunnen gebruiken. False-positives moeten worden gemitigeerd door enerzijds optioneel contextuele informatie van een contact op te slaan en anderzijds door kwaadwillende actoren buiten te houden. Contextuele informatie kan ook helpen het risico op besmetting te duiden. De gebruiker helpen risicovolle contacten te verminderen, door te waarschuwen bij <1.5 meter afstand en per dag statistiek van risicovolle contacten te tonen. Ook moet de gebruiker beschermd worden voor inmenging van derde partijen, zoals de werkgever.

### 3. Procesmatige borging - kwaliteit software ontwikkeling, adoptie en continue monitoring

Voor 28 april analyseren wij of good practices gevolgd zijn conform NCSC- en AP-richtlijnen en adviezen vanuit tracing initiatieven zoals DP-3T en PEPP-PT. Parallel bekijken we of een robuust ontwikkel- en quality assurance proces is gehanteerd in lijn met ISO 12207. Aanvullend analyseren we in hoeverre waarborgen (conform o.a. OWASP SAMM) zijn ingebouwd om veilige en effectieve verwijdering van data mogelijk te maken. Naar aanleiding van deze analyses zullen we concrete aanbevelingen maken.

Essentieel in de aanpak is de gebruikerservaring, die leidt tot adoptie in de samenleving. Wij zullen u adviseren hoe de digitale oplossing intuïtief, doelgericht, en eenvoudig in het gebruik zijn zodat adoptie gemaximaliseerd wordt en zullen hierover adviseren.

Samen met u zorgen wij dat we in control zijn en bij incident weer snel in control komen en blijven doordat wij u continu inzicht geven in risico's, adviseren over maatregelen en helpen de belangrijkste maatregelen te meten, monitoren en evalueren. Ook het ontwerpen van KPI's alsmede het toetsen van de kwaliteit van data en ontwerp van algoritmes (*responsible AI*) doen we. Op basis van continuous monitoring meten we aanpassingen in instellingen, controles en opvolgacties om kwaliteit van data en algoritmes te borgen.

#### 4. Technische borging - bewezen innovatieve testmethode en diepe kennis

Onze innovatieve en bewezen testmethode, geoptimaliseerd met machine learning-technieken, test de beveiliging van de digitale oplossing in minder tijd en met meer diepgang. Dit draagt bij aan snelheid van de uitrol, maar ook vertrouwen vanuit de maatschappij (voor en na uitrol doorlopend testen). Bij technische beveiliging van de gegevens zijn drie zaken van belang:

- Security en kwaliteit van de digitale oplossing en de broncode: met onze continue penetratietest services monitoren wij kritische omgevingen voortdurend op kwetsbaarheden en wijzigingen. De service is schaalbaar en zeer effectief. Via architectuur analyse en broncode review analyseren we voor 28 april of de oplossing conform ISO 25010 eisen gebouwd is en de architectuur robuust is. Tevens analyseren we cryptografische kwaliteit en opzet en mate van bestand zijn tegen aanvallen.
- Beveiliging API's en technische privacy implementatie: wij verwachten dat gebruik gemaakt wordt van gestandaardiseerde en open-source API's. Wij zullen voor 28 april penetratietesten uitvoeren op deze API's en testen of er geen, naar personen herleidbare, gegevens worden meegestuurd.
- Transmissie van gegevens en encryptie: de oplossing maakt gebruik van servers, waarop (in het geval van DP-3T) de gegevens worden opgeslagen, zoals de geïnfecteerde ID's. De integriteit en vertrouwelijkheid van deze data zijn randvoorwaardelijk. Wij testen de beveiliging van de servers, maar ook de encryptie van de verbindingen en de data zelf. Daarnaast bekijken we, vanuit het perspectief van een aanvaller, de mogelijkheden tot het vervuilen of beschadigen van de data en de risico's om vanuit versleutelde interacties gevoelige informatie te deduceren.

Onderdeel van ons team is de externe expert 5.1.2e een aan PwC verbonden hoogleraar cryptografie en security management.

#### 5. Juridische borging - nationaal en internationaal perspectief

Vertrouwen in een digitale oplossing vraagt een sterke juridische basis. We monitoren proactief de ontwikkelingen vanuit diverse (inter)nationale toezichthouders. Onze juridische analyse en advies richt zich op:

- Privacy en rechten van individuen: het toepassen van juridische vereisten (rondom o.a. toestemmingsverzoeken, dataminimalisatie, minderjarigen en gelaagde notificaties). Daarnaast adviseren we over de melding en communicatie van eventuele datalekken en analyseren we bestaande DPIA's of voeren nieuwe DPIA's uit.
- Verantwoordelijkheden: de rol en verantwoordelijkheden van VWS bij het inrichten van een verwerkingsregister, dataminimalisatie, dataretentie en -vernietiging en het delen van gegevens met derden. Wij adviseren vanuit privacy- en gezondheidsrecht. We geven specifieke aandacht aan Privacy by Design, pseudonimisering/anonimisering en Privacy Enhancing Technologies.
- Relevante stakeholders: de governancestructuur, zodat betrokkenheid van relevante partijen (zoals toezichthouders) mogelijk is, maar ook een onafhankelijke gegevensbescherming rol. Daarnaast bieden wij advies bij het opstellen en beoordelen van vereiste contracten en protocollen en van gedocumenteerde afspraken met (lagere) overheden.