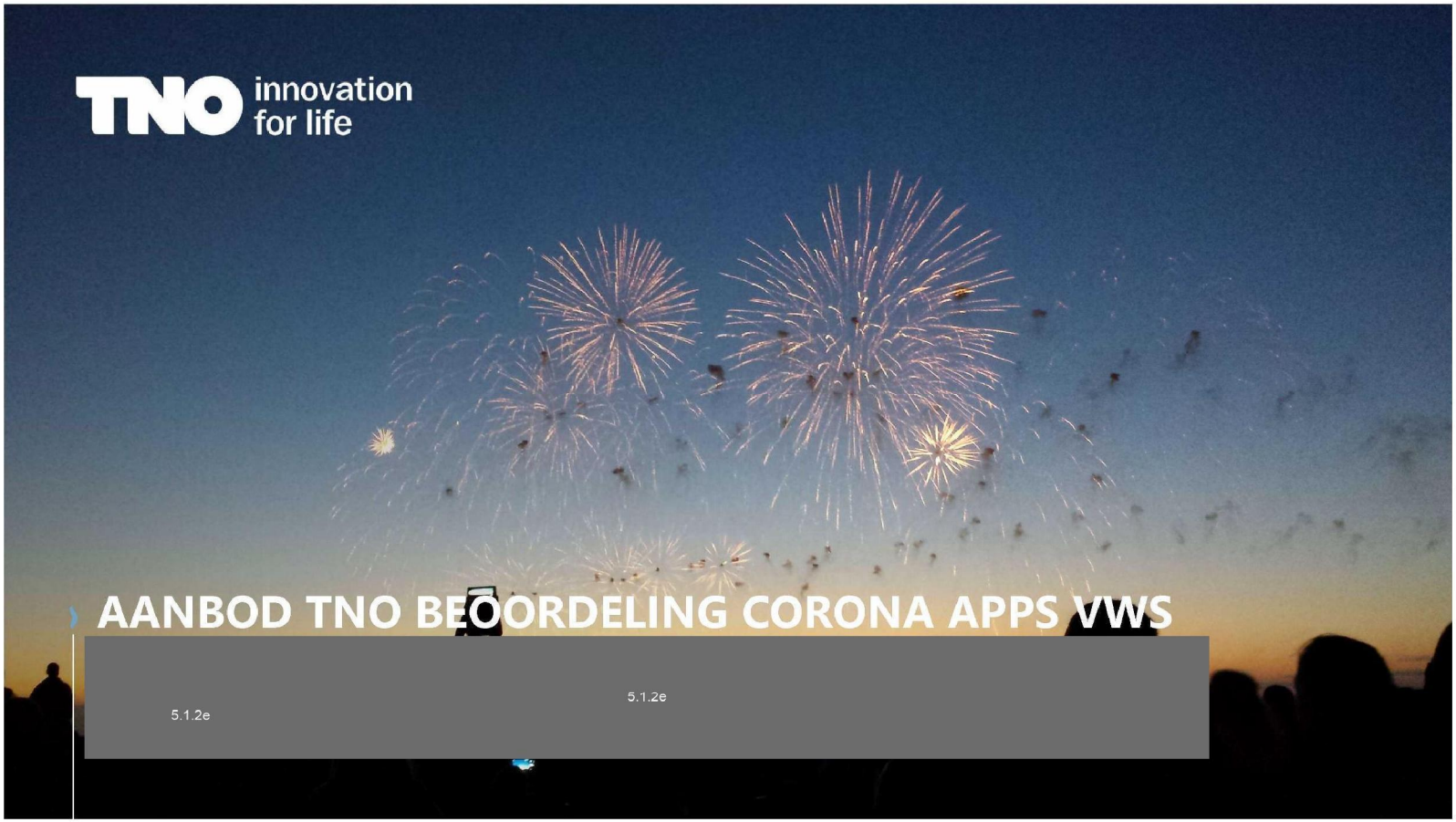
TNO innovation for life
AANBOD TNO BEOORDELING CORONA APPS VWS
5.1.2e
5.1.2e

AANBOD
VAN TNO AAN VWS

Wat bieden we aan:

- **Expertise** zowel binnen TNO als via TNO's uitgebreide (inter)nationale expert netwerk, in te zetten voor:
  - Het **adviseren** van beslissers
  - Het formuleren en/of toetsen van **requirements**
  - Het **beoordelen** van aanbiedingen

Wat maakt TNO bijzonder:

- Passend bij de **wettelijke taak** van TNO
- **Onafhankelijk:** TNO heeft geen commerciële belangen bij een app
- Brede **multidisciplinaire wetenschappelijke** kennis (beta/gamma: zowel techniek als gebruiker/maatschappij)
- **Ervaring** in het coördineren en programmeren van toegepast wetenschappelijk onderzoek samen met veel belanghebbenden: overheden, private en academische partners
- Beschikbaarheid van een groot (inter)nationaal **netwerk** van experts op alle relevante aspectgebieden.

TNO innovation for life

9 EXPERTISEGEBIEDEN
VAN BELANG VOOR HET INTRODUCEREN VAN EEN COVID-19 APP

- Technisch
  - Hoe werkt de app en hoe is deze ontworpen? Kan de app miljoenen gebruikers maandenlang aan?
- Data en privacy
  - Waar wordt welke data opgeslagen en verwerkt, wat is de impact op privacy, is dat wel veilig?
- Security
  - Hoe zien de risico's er uit bij gebruik van de app, hoe is de vertrouwelijkheid van de data geregeld en kunnen we wel garanderen dat de data (blijven) kloppen?
- Testing
  - Bruikbaarheidstests en technische tests
- Effectiviteit
  - Gaat de app ons inderdaad de inzichten opleveren die we nodig hebben?
- Sociale implicaties
  - Zijn er kansen dat bepaalde groepen benadeeld worden? Gaat iedereen de app (willen) gebruiken? Hoe kun je het gebruik bevorderen
- System governance
  - Wie is de eigenaar van het systeem, en hoe transparant is de app?
- Data governance
  - Hoe wordt omgegaan met het bewaren van gegevens, en het verwijderen als mensen er mee stoppen of de app niet meer nodig is? Hoe houd je bij wat het werkelijk gebruik van de app is?
- Best practices wereldwijd
  - Welke ervaringen zijn er met vergelijkbare apps, en wat leren wij daaruit over het vermijden van valkuilen?

TNO innovation for life

TECHNISCHE ARCHITECTUUR

- Wat is het **systeemconcept**?
  - Is er sprake van een centrale server? Welke eisen zijn daaraan te stellen, waar staat deze?
  - Welke componenten zitten er in het system (app, server, browsers, ...)
  - Wordt locatiebepaling toegepast, en zo ja, hoe? (GPS, telecomnetwerk, WiFi AP herkenning, ...)
- Wat is de **robuustheid** van het systeem (zowel de app als een eventuele centrale server)?
  - Kan het system grote volumes aan? Blijft het goed werken als er miljoenen gebruikers maandenlang gebruik van maken?
- Welke **devices** worden ondersteund?
  - Android, iOS, anders; welke hardware moet in die apparatuur zitten?
- Wat is de **communicatie-architectuur**?
  - Peer-to-peer en/of gecentraliseerd; hoe vaak; op welke manier (protocol)
  - Welke radiocommunicatietechologie(ën) worden toegepast (BlueTooth, wifi, mobiele netwerk)
  - Met welke servers wordt gecommuniceerd? (bv. centrale datacollectie, zorgverleners)

DATA EN PRIVACY

- De omgang met data is de Achilleshiel van de app!

- Onderwerpen waar op gelet moet worden
  - Hoe is de **opslag van de data** geregeld: waar wordt deze opgeslagen, hoe wordt de opslag beveiligd, wat wordt er precies opgeslagen
  - Hoe wordt de data **verwerkt**: waar wordt deze verwerkt (op een server of op het apparaat van de gebruiker)
  - Hoe wordt de **Privacy Impact Assessment** gedaan en door wie?
  - Welke **algoritmes** worden bij de verwerking ingezet? Weten we hoe die werken?
  - Welke **app-permissies** zijn nodig? Geeft de gebruiker toestemming (AVG)?
  - Wordt de data **geanonimiseerd** opgeslagen? Wat zijn de mogelijkheden voor re-identificatie?
  - Kan de data worden **verwijderd**?

SECURITY (1)

- Risico-analyse als basis voor de security architectuur
  - Uitwerken dreigingen, risicobeoordeling, beschermingsmaatregelen en restrisico's
- Security governance
  - Security verantwoordelijkheden helder beleggen
  - Security monitoring (identificatie, analyse van security events)
  - Incident response (inrichten organisatie en proces)
- Autorisatie
  - Welke gebruikersrollen? (eindgebruiker, zorgverlener, overheid/RIVM?)
  - Welke functionaliteiten? ((de-)activatie app, informatie-uitwisseling met ander device, met server, wijzigen gebruikersprofiel, wijzigen van de gezondheidsstatus van een gebruiker, ...)
  - Wie kan wat? Mapping van functionaliteiten op gebruikersrollen

SECURITY (2)

- Authenticatie
  - Onderscheid kunnen maken tussen gebruikers
  - Is multi-factor authenticatie mogelijk (meer dan alleen wachtwoord)
  - Server-authenticatie (vertrouwd (overheids-) certificaat)
- Integriteit van de app
  - Evt. kwetsbaarheden opsporen via code review of penetratie testing
  - Awareness bij gebruikers om alleen via vertrouwde app stores te downloaden
- Integriteit en vertrouwelijkheid data
  - In opslag (on-device, op centrale server) en terwijl deze verstuurd wordt (bv SSL)
- Assurance: Logging / audit trail
- Beschikbaarheid
  - Kan de server blijven draaien? Denk aan load balancing / DDoS preventie
  - Fail-safe gedrag bij wegvallen connectiviteit (m.n. geen verlies/compromittering van data)

USABILITY EN TECHNISCHE TESTING

- Het effectief gebruik van elke nieuwe technologie staat of valt met het **bruikbaarheid** (usability).
- Een goede **usability test** vóórdat een app uitgerold wordt is essentieel.
- TNO heeft zeer uitgebreide ervaring met usability
  - De meest recente **wetenschappelijke inzichten**
  - Ervaring met het doen van **usability tests**; TNO beschikt over een grote lijst proefpersonen
- **Andere tests** naast usability tests:
  - TNO heeft ervaring met testing: lab-testen en *in-situ* testen
  - Er is momenteel een initiatief met Gem. Amsterdam en EZK om een app testomgeving op te zetten, hier kan eventueel op aangesloten worden

TNO innovation for life

EFFECTIVITEIT

- De **effectiviteit** van de app is één van de belangrijkste aspecten!

- Aspecten bij het beoordelen van effectiviteit
  - **Minimaliseren van missers**: de kans op zogenaamde 'false positives' en 'false negatives'
  - **Verstorende technische belemmeringen** (kenmerken van de smartphones, andere apps, stoorsignalen, onderscheid maken in signalen van verschillende andere apparaten)
  - Invloed van de app op het **functioneren van de smartphone** (als deze bijvoorbeeld veel batterij gebruikt dan zullen gebruikers de app eerder verwijderen)
  - **Proportionaliteit**: alleen bij een minimum dekkingsgraad en daarmee effectiviteit is de inzet, en de (mogelijke) inbreuk op privacy gerechtvaardigd

SOCIALE IMPLICATIES

Mogelijke sociale implicaties van het toepassen van apps om enerzijds de ontwikkeling van het ziektebeeld van Covid-19 slachtoffers te kunnen volgen en op basis daarvan de behandelstrategieën te verbeteren en hen te adviseren, en anderzijds diegenen die in de nabijheid van deze patiënten zijn geweest te informeren en adviseren:

- Sociale adoptie en dekkingsgraad: Welke bevolkingsgroepen zijn bereid deze apps te gebruiken en wat zijn daarvan de consequenties voor de vereiste/gewenste dekkingsgraad nodig om effectief te kunnen worden gebruikt. Kan deze dekkingsgraad worden bereikt door vrijwillige adoptie? Of zijn vormen van dwang nodig en welke vorm(en) van toezicht en handhaving zijn in dat geval in te richten en wat is daarvoor benodigde inspanning, gelet op de acceptatie daarvan, cq draagvlak daarvoor.

- In welke mate leidt het gebruik van deze app(s) tot (on)gewenste profilering, en mogelijke sociale uitsluiting
- Welke oplossingen zijn denkbaar voor personen die wél bij willen dragen, maar geen smartphone app kunnen of willen gebruiken?

- Incentives: welke mogelijke voordelen levert het gebruik van de app(s) de gebruikers ervan en wegen die voldoende op tegen de potentiële nadelen voor deze gebruikers.

- Wat zijn de kansen op misbruik (misplaatste grappenmakerij, aanknopingspunten voor phishing, ...)

TNO innovation for life

SYSTEM GOVERNANCE

- Wie is de **eigenaar** van het systeem?
  - Wie kan en mag besluiten over de functionaliteit, de status, de updates, het 'aanzetten' en 'uitzetten'
  - Hoe worden updates getest, goedgekeurd en uitgerold?
  - Hoe zijn de besluitvormingsprocedures geregeld?

- Transparantie:
  - Het gebruik van de app en de daarmee gepaard gaande data-uitwisseling en –verwerking kent een aantal mogelijk risico's met name op het terrein van cyber- en data-veiligheid.
  - Het vertrouwen van de samenleving is gebaat bij een vorm van transparantie waarbij vastgesteld moet worden transparantie van wát (hele systeem, algoritme, ...), voor wie, en voor welk doel.
  - Deze transparantie kan volledig zijn, bijvoorbeeld door gebruik van open source, of procedureel door disclosure aan een trusted third party.

DATA GOVERNANCE

- Data governance: om de app te laten werken zal de door deze app gegenereerde data moeten worden verzameld en verwerkt. Afhankelijk van de gekozen transmissie en data-opslagstrategie is sprake van grotere dan wel minder grote risico's met betrekking to privacy, cyber- en data-veiligheid. In dit kader zal ondermeer gedacht moeten worden aan de volgende zaken:
  - Afschalingsproces (vgl GRIP niveau): Het verzamelen en verwerken van de door App(s) gegenereerde data kan in de huidige (nood)situatie wellicht worden gerechtvaardigd, maar het is zaak nu reeds rekening te houden met toekomstige afschaling en daarmee inperking daarvan.
  - Retentie: Hoe lang zouden de gegevens gelet op rechtmatig en doelmatig gebruik van de gegevens opgeslagen moeten worden en hoe kan, eventueel na afschaling, het in AVG vastgelegde 'right to be forgotten' worden geëffectueerd.
  - Monitoring op eigenlijk gebruik: Op welke manier kan het rechtmatig gebruik van de app, de door deze app gegenereerde gegevens, de gegevensverzameling en -verwerking worden gemonitord en oneigenlijk gebruik worden voorkomen

BEST PRACTICES

- In Nederland zijn er inmiddels **tientallen aanbieders** van mogelijke oplossingen
- In **Europa** zijn er verschillende apps in gebruik of worden deze onderzocht
  - Standaardisatie, of onderlinge uitwisselbaarheid (internationale reizigers!) wordt ook van belang
- Ook **buiten Europa** zijn er veel voorbeelden, alhoewel die ervaringen door een andere sociale structuur niet één op één over te zetten zijn naar Nederland

- TNO heeft een uitgebreid **internationaal netwerk**, met name in Europa:
  - **Collega-onderzoeksorganisaties** zoals Fraunhofer (D), INRIA (F), VTT (FI) en alle grote universiteiten
  - Andere Europese **telecombedrijven** die soms een rol spelen met hun netwerkgegevens
  - Bij de **Europese Commissie** waar nu (ook) veel initiatieven worden ingediend
  - De 200 leden van de **Big Data Value Association**
- **Inzichten en ervaringen** uit dit netwerk kunnen we in Nederland gebruiken


BEDANKT VOOR
UW AANDACHT
TNO innovation for life