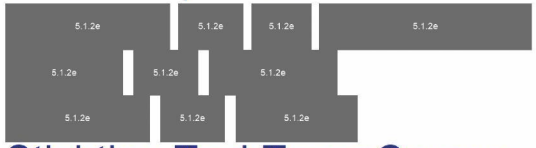
Digitale Tools

04/02/21 | 11:00

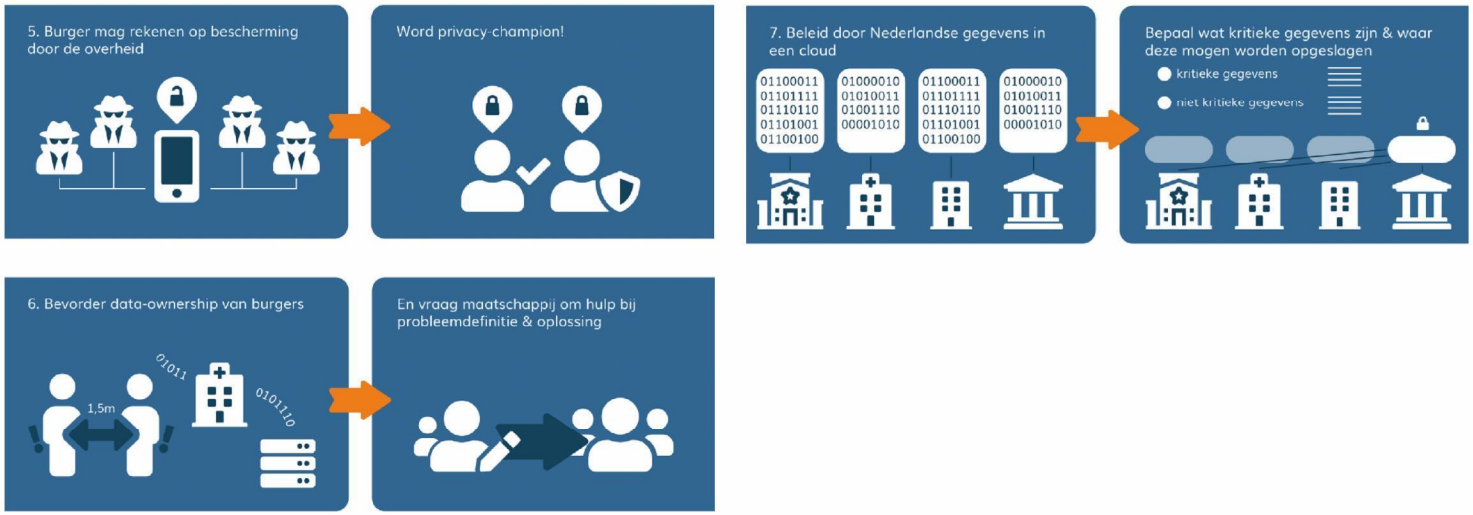


Stichting TechTegenCorona
www.techtegencorona.nl

TECH TEGEN CORONA

Advies Digitale Tools van de Overheid

Advies Digitale Tools van de Overheid



Wat ging goed?

Corona-
Melder App

De ‘mislukking’ van de Appathon was een blessing in disguise.

Hierdoor kreeg de samenleving de kans om niet alleen na te denken over de *oplossing* (“kies & beoordeel de gemaakte covid-apps”) maar over de *vráágstelling* (“wát is er eigenlijk nodig? Een covid-app die open-source, privacy-vriendelijk enz enz is.

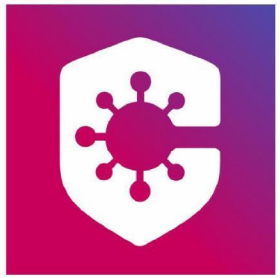
Deze manier wordt nu ook gebruikt voor de GGD-app: de leden van o.a. CodeForNL worden continu om advies gevraagd.

Lessons learned: betrek burgers niet bij de ‘eindfase’ van data-tools maar vanaf het eerste begin: de bepaling van de vraag.

Wat kon er beter?

Corona-
Melder App

De daadwerkelijke uitrol van de CoronaMelder duurde langer dan verwacht, om meerdere redenen. Vooropgesteld: te midden van de pandemie moest het desbetreffende departement op meerdere borden tegelijk schaken. Twee belangrijke *lessons learned:*



Nieuwe wetgeving vereist

Nieuwe data-tools vereisen in een gedigitaliseerde versie steeds vaker aparte wetgeving.

Beperkte controle over Google-Apple API

Waarschijnlijk zou het mogelijk zijn geweest om hulp te vragen aan andere departementen (bv BZK) om in Europees verband te pleiten voor aanpassingen in de Google-Apple API

Datastrategie voor 1,5 m samenleving

Sinds de start van de pandemie neemt de data-vergaring door (verschillende lagen) van de overheid toe. Door de complexe (crisis) organisatie zijn dubbelingen –en hiaten- vaak onbekend.

Vertrouwen 🤝

De grootste uitdaging voor data-tools van de overheid is het vertrouwen van de burger. Om deze reden is het cruciaal om aan te geven waarom bepaalde data worden verzameld/gekoppeld en deze ook uitsluitend voor dat doeleinde te gebruiken. Ook is transparantie over de opslag en opslag-termijnen cruciaal.

Zorg er actief voor dat mensen vertrouwen kunnen hebben in het gebruik van data, o.a. door actief onderwijzen.

Hou tools zo eenvoudig mogelijk; voorkom Pandora's box

De politie probeert nu te begrijpen welke algoritmen er in hun tools zitten. Met als streven om 'pandora's boxes' niet meer te gebruiken.

Overheid; doe het niet (allemaal) zelf

Een deel van de overheid heeft van oudsher nog een mentaliteit dat ze het zelf graag doen. Maar juist in deze tijden met een extreem snelle digitale transformatie is samenwerking met andere actoren belangrijk

Data & Veiligheid

Data en veiligheid hebben een interessante wisselwerking met elkaar:

- Zo kan data zorgen voor een hogere mate van veiligheid. Een voorbeeld hiervan is het Corona Dashboard die covid-19 data bij elkaar brengt.

- Maar ook de veiligheid van Nederland **verlagen.** Door bijvoorbeeld het verzamelen van kritische/gevoelige gegevens loopt het dashboard mogelijk meer risico om gehackt te worden.

1

Defensie ziet verschillende aspecten van data:

1) Technische aspect: besteed meer aandacht aan het beschermen van data voor cruciale systemen, zoals wapens maar ook patiëntendossiers.

2) Interoperabiliteit aspect: richt systemen zo in dat externe partijen kunnen controleren of de data die deze netwerken genereren en versturen klopt.

3) Ethische aspect: ook al gaan andere landen of bedrijven rücksichtsloos om met data; blijf vast houden aan de moral high ground. Geen compromissen sluiten omdat anderen dit wel doen.

Privacy en data-ownership

Wees eerlijk over data-bloopers; dat verhoogt (uiteindelijk) het vertrouwen van burgers

Bij het bouwen van data-tools kost het veel meer moeite om ze privacy-vriendelijk te maken. (Nederlandse zoekmachine heeft er **anderhalf jaar langer** over gedaan om alle intrusive-by –design subonderdelen te slopen)

Overheid: neem de lead in het verbinden van data aan privacy en de Grondwet. Nederland zou als grootste Europese data-knooppunt de Europese data-privacy champion kunnen worden.

En moedig ambtenaren aan om zelf zoveel mogelijk privacyvriendelijke tools te gebruiken op hun telefoons, laptops, enz.

Tot slot: burgers hebben op dit moment te weinig mogelijkheden om privacy en veiligheid bij data-tools af te dwingen. De Nederlandse overheid zou burgers meer kunnen bijstaan in het streven naar dataownership.

Data & Gezondheid

Gezien de snelle ontwikkelingen op het gebied van MedTech is het van belang om meer richtlijnen te bieden aan de zorginstellingen m.b.t. data & veiligheid. De veiligheid van de medische datatools wordt met name bewaakt door private partijen.

Wat zorginstellingen niet altijd beseffen is dat veel zorgleveranciers slechts datatools plaatsen. Zij vermelden er niet bij dat de beveiliging erbij moet worden gekocht. Dit leidt ertoe dat de ziekenhuizen in Nederland niet goed beschermd zijn.

Dit bleek uit een onderzoek van Cybersprint. Zij onderzochten in totaal 7258 websites, servers en IP-adressen van de acht academische, de tien grote en de tien kleinste ziekenhuizen. Bij alle ziekenhuizen stelden zij kwetsbaarheden vast

Data & Gezondheid

De invoering van centrale EPDs is efficiënter voor patiënten en medewerkers. De ervaring leert echter dat zorginstellingen te snel patiëntengegevens met externe partijen delen. Om ervoor te zorgen dat er wel veilig met de data wordt omgegaan moet er strengere wet- en regelgeving komen m.b.t. het beschermen van de persoonsgegevens van patiënten.

Nieuwe data-tools: van wie zijn de gegevens?
Toename aan gezondheids-apps, ook van ziekenhuizen, zorgverzekeraars en commerciële zorginstellingen. In sommige gevallen worden data verhandeld zonder dat de burger zich hiervan bewust is.

Tot slot: zorginstellingen moeten transparant zijn naar hun patiënten en aangeven:
- Welke data van hen wordt opgeslagen;
- Waar de data voor worden gebruikt;
- Hoe lang de data wordt opgeslagen

Tot slot: selectie van paar punten

"Te midden van covid-19 waren tal van (semi)overheidsorganen genoodzaakt om snel te handelen en data ergens op te slaan.

Terugblikkend kan worden geconstateerd dat het cruciaal is om te bepalen welke data van Nederlandse burgers waar – en in welke hoeveelheid – wordt opgeslagen. Wat zijn kritieke data – en wat niet?

Patiëntendossiers in combinatie met BSN-nummers en/of juridische dossiers en/of andersoortige privacygevoelige informatie dan wel een accumulatie van gegevens dienen niet toegankelijk te zijn voor buitenlandse actoren. "

Aanbevelingen

Betrek het maatschappelijk middenveld vanaf de allereerste fase: het definiëren van het probleem.

Als zevende dataknooppunt van de wereld; neem de lead in data & democratie.

Van informatiemonopolie naar informatiedeling.

Vraag de Nederlandse maatschappij om hulp voor het verbeteren van dataownership en het oplossen van wicked problems.

Reflectie over kritieke gegevens en het opslaan in de (internationale) cloud.