CRITERIA VOOR TECHNOLOGISCHE OPLOSSINGEN

2020-04-10 – Coalitie Veilig tegen Corona

1. Eén doel

a. Doelbinding: De oplossing adresseert een helder omschreven probleem en een helder omschreven doelgroep.

b. Toezicht: Ander gebruik van de oplossing en eventueel gegenereerde data is verboden en wordt voorkomen. Dus ook gebruik in het kader van strafvorderlijk onderzoek of in het kader van inlichtingen- en veiligheidsdiensten. Desnoods door een tijdelijke beleidsregel van het OM en de inlichtingen- en veiligheidsdiensten. Vertrouwen van burgers is hier essentieel, dit vertrouwen mag niet beschaamd worden.

- Voorbeeld: Een applicatie mag bijvoorbeeld niet gebruikt worden voor de handhaving van beleid, voor het bepalen of iemand in aanmerking komt voor een vergoeding van of toegang tot zorg of voor commerciële doeleinden.
- Voorbeeld: de applicatie mag uitsluitend gebruikt worden voor de preventie van COVID-19, het opsporen van besmettingsgevallen van COVID-19 en het bijbehorende contactonderzoek.

2. Gebaseerd op wetenschappelijk en maatschappelijk inzicht en bewezen effectief.

a. Onderbouwd: De inzet van de dienst en eventuele verzamelde data moet gebaseerd zijn op wetenschappelijke kennis, maatschappelijke validatie en aantoonbaar bijdragen aan het onder controle krijgen van het virus. De makers tonen bewustzijn van gelijksoortige initiatieven en leggen uit hoe eerder opgedane inzichten (binnen en buiten Nederland) zijn meegenomen in het ontwerp. Bij de onderbouwing wordt gebruik gemaakt van zowel epidemologische inzichten, de GGD-praktijk, sociale aspecten als de state-of-the-art van privacy-by-design.

b. Meetbaar: Het is helder welke factoren van belang zijn voor de effectiviteit van de dienst.

c. Getest: De dienst is vooraf getest met een beperkte groep gebruikers, op basis waarvan aantoonbaar is dat deze dienst noodzakelijk, effectief en proportioneel is.

d. Voortdurende evaluatie van de dienst waarbij effectiviteit aantoonbaar moet zijn. Bij gebrek daaraan wordt de dienst ge-de-activeerd

- Voorbeeld: Het is gespecificeerd hoeveel mensen de dienst moeten gebruiken om hem effectief te laten zijn.

3. Bewezen betrouwbaar en vanuit expertise.

a. Expertise: De betrokkenen hebben relevante expertise in de domeinen waar de dienst aan raakt.

b. Interdisciplinair en divers: Interdisciplinaire en diverse teams zijn beter in staat om vraagstukken in kaart te brengen en dragen betere oplossingen aan.

c. Open en transparant: Naast deskundigheid is ook open ontwerproces, participatie, publieke verantwoording en transparantie van de dienst noodzakelijk.

d. Mensenrechtelijk kader: De dienst bevordert mensenrechten en democratische beginselen.

e. Open source: De broncode van de applicatie en de overige infrastructuur is vanaf de start openbaar toegankelijk, toetsbaar en de dienst is reproduceerbaar op basis van de broncode. Naast de broncode worden ook de ontwerpdocumenten, zowel functioneel als technisch, en de API-specificaties openbaar gemaakt.

f. Vrije software: De broncode van de applicatie en de overige infrastructuur wordt gepubliceerd onder een vrije software licentie

g. Data commons: Voor zover er niet-persoonlijke data wordt gegenereerd wordt deze in een data commons of data trust ondergebracht en onder publiek toezicht geplaatst.

- Voorbeeld: Als de oplossing gebruikt moet worden door een aanzienlijk deel van de bevolking, mogen we op geen enkel moment in de ontwikkeling en inzet van de applicatie juridisch afhankelijk zijn van één enkele partij of systeem.
- Case: https://standard.publiccode.net/

4. De inzet van de dienst is per definitie tijdelijk.

a. De oplossing mag alleen worden ingezet voor het vooraf gespecificeerde doel en voor een vooraf bepaalde termijn. Enkel en alleen indien aantoonbaar noodzakelijk is dat de dienst langer wordt gebruikt, kan deze termijn worden verlengd.

b. Als de dienst niet meer effectief of noodzakelijk is, wordt de uitrol teruggedraaid en wordt de data verwijderd. Dit kan ook indien er maatschappelijke onrust ontstaat, bijvoorbeeld omtrent veiligheid of mogelijk misbruik van de dienst. Terugdraaien kan door de functionaliteit van de dienst ongedaan te maken en de geregistreerde gegevens te verwijderen.

5. Niet tot individuen herleidbaar.

a. Anoniem: Wanneer persoonsgegevens verwerkt worden, moet het onmogelijk zijn om met deze gegevens gebruikers te de-anonimiseren, ook niet als de gegevens worden gecombineerd met andere gegevens.

- Voorbeeld: Een contactonderzoek-app mag niet gebouwd zijn op het gebruik van identificatienummers van hardware of andere identificerende gegevens, zoals het "Bluetooth Device Address".

- Case: vluchtige identificatienummers, zoals bijvoorbeeld in DP-3T, waarbij het mogelijk is contacten te reconstrueren zonder surveillance te hebben die voor andere doelen ingezet kan worden.

6. Zo min mogelijk gegevens worden gebruikt.

a. Dataminimalisatie: De dienst slaat zo min en zo kort mogelijk gegevens op. Er is geen centrale infrastructuur waarin gegevens uit de app worden uitgelezen. Dit geldt ook voor gebruiksstatistieken of andere app-feedback; dit is enkel toegestaan indien het epidemiologisch van belang is.

- Voorbeeld: Een contactonderzoek-app hoeft geen gegevens over iemands locatie vast te leggen, maar slechts het tijdelijke 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.

7. Geen centraal opgeslagen persoonsgegevens.

a. Alle gegevens en processen worden in beginsel lokaal op het apparaat van de gebruiker zelf verwerkt.

b. Gegevens mogen uitsluitend uitgelezen of gedeeld worden als er sprake is van a) contact- of brononderzoek als bedoeld in art. 6 Wpg, of b) toestemming van de gebruiker.

c. Gegevens die wél het apparaat van een persoon verlaten, mogen op geen enkele wijze iets zeggen over het verplaatsingsgedrag, tijdstip, locatie of sociale netwerk van die persoon.

- Voorbeeld: In het geval van een contactonderzoek-app vindt het proces van de beoordeling of een gebruiker recent in contact is geweest met een besmet persoon, bij de gebruiker plaats.
- Case: DP-3T: https://github.com/DP-3T
- Case: Signal: https://signal.org/
- Case: My Data Done Right: https://mydatadoneright.eu

8. Veilig en bestand tegen misbruik.

a. Non-discriminatoir: risico's op uitsluiting of oneerlijke behandeling zijn in kaart gebracht en er wordt overtuigend uitgelegd hoe deze risico's worden ondervangen, in het bijzonder de kans op stigmatisering door het hebben van een positieve COVID-19-status.

b. Integriteit en vertrouwelijkheid: Het is belangrijk dat de vertrouwelijkheid en integriteit van gegevens beschermd worden. Dat kan door het gebruik van encryptie en andere beveiligingstechnologiën. Soms is meer nodig. Denk bijvoorbeeld aan een

situatie waarin de app enkel bij de constatering van een besmetting een seintje geeft aan een andere gebruikers. Versleuteld of niet, uit de verzending van gegevens is al af te leiden dat de desbetreffende gebruiker mogelijk besmet is.

c: Geaudit: Opzet, bestaan en werking worden gecontroleerd door (bij voorkeur meer dan één) auditerende partij. Zowel voorafgaand aan de lancering als op regelmatige basis totdat het systeem definitief wordt uitgeschakeld. Ook ziet zij erop toe dat uiteindelijk alle verzamelde gegevens en toestemmingen permanent worden verwijderd.

d: Meldpunt: er moet een adequaat meldpunt beschikbaar en eenvoudig te bereiken zijn waarop meldingen van fouten en kwetsbaarheden in ontwerp en implementatie gemeld kunnen worden. Het moet helder omschreven zijn binnen welke termijn en op welke wijze er terugkoppeling wordt verleend en bevestigde fouten en kwetsbaarheden verholpen zijn. Melders moeten beschermd zijn middels een responsible disclosure-beleid en hebben het recht tot onvoorwaardelijke publicatie van hun bevindingen.

9. Gebruiksvriendelijk en toegankelijk.

a. Makkelijk in het gebruik: Het ontwerp en de functionaliteit van de oplossing sluit aan bij de beoogde doelgroep. In het geval van een brede doelgroep wordt in het bijzonder aandacht besteed aan het gebruik van de oplossing door kwetsbare groepen.

b. Toegankelijkheid: Iedereen kan de dienst gebruiken, los van technologische of persoonlijke beperkingen.

c. Maatwerk: Een goede digitale oplossing voor iedereen is niet hetzelfde als één oplossing voor iedereen.

d. Co-creatie: De doelgroep(en) waarop de dienst betrekking heeft, wordt betrokken bij het maakproces.

e. Interoperabiliteit: Interoperabiliteit verhoogt de kans op aansluiting bij een zo groot mogelijke groep en stimuleert innovatie.

- Good practice: Small Tech Foundation: https://small-tech.org/a
- Good practice: Glitch: https://glitch.com/

10. Gebruik van de dienst mag onder geen beding onder dwang van overheid of derden plaatsvinden, en nooit een voorwaarde voor deelname aan algemeen maatschappelijk verkeer kunnen zijn.

a. Keuzevrijheid: Het gebruik van de dienst mag op geen enkele manier worden afgedwongen. De keuze om een dienst niet te gebruiken is er altijd.

b. Geen stimulans: Personen mogen ook met bijvoorbeeld een financieel lokkertje niet worden gestimuleerd om de dienst te gebruiken.

c. Pauze: In geval van een gedownloade applicatie, moet deze tijdelijk uit te schakelen en permanent te verwijderen zijn.

d. Geen consequenties: Aan het weigeren van het gebruik mogen geen negatieve consequenties verbonden zijn. Dat betekent dat ook andere partijen, zoals een luchtvaartmaatschappij, zorgverzekeraar of een restaurant, geen negatieve dan wel positieve gevolgen mogen verbinden aan al of niet gebruik van de app. Dit geldt ook voor de gevallen waarin het niet gebruikt kán worden, zoals voor mensen die geen smartphone bezitten.

e. Machtsrelaties: In het bijzonder moet het gebruik door werkgevers jegens werknemers en door opleidingsinstanties jegens scholieren/studenten strikt verboden worden.