Advies 23: (Informatie)veiligheid en gebruik CoronaCheck

Begeleidingscommissie Digitale Ondersteuning Bestrijding Covid-19

26 juli 2021

Inleiding Begeleidingscommissie

De Minister van Volksgezondheid, Welzijn en Sport (VWS) heeft een Begeleidingscommissie ingesteld die de Minister zal adviseren over digitale ondersteuning bij de bestrijding van Covid-19. De begeleidingscommissie brengt naast gevraagde adviezen ook ongevraagde adviezen uit. Onderstaande betreft een advies over de (informatie)veiligheid en gebruik van de CoronaCheck app.

In zeer korte tijd zijn gedurende deze pandemie op verschillende manieren veel data van burgers verzameld in het kader van de bestrijding van de pandemie. In navolging op eerder gegeven formele (o.a. adviezen 19 en 22) en informele adviezen, en naar aanleiding van het recente datalek bij een commerciële testaanbieder adviseert de commissie wederom een aantal essentiële aandachtspunten ter bevordering van de (informatie)veiligheid van de CoronaCheck app en de verbindingen die deze maakt met achterliggende databases, o.a. van commerciële testaanbieders.

(1) Meer regie op toezicht commerciële testaanbieders

Zoals ook in onze eerdere vele formele en informele adviezen door de commissie aangegeven[1] hecht de Begeleidingscommissie zeer aan de veiligheid van de CoronaCheck app en met name aan beveiliging van de verbindingen naar de gebruikte bronsystemen van o.a. het RIVM (CIMS), de GGD en ook commerciële testpartijen. Het recente datalek bij een van de commerciële testaanbieders heeft nog eens aangetoond hoe kwetsbaar deze verbindingen zijn, juist omdat het gaat om gevoelige persoonsgegevens.

De commissie wil meegeven dat VWS niet alleen vooraf maar ook na de aansluiting met grote regelmaat moet laten controleren of deze partijen nog steeds voldoen aan de gestelde eisen en adviseert de minister om daar nog meer regie te nemen. De CoronaCheck app zelf, maar met name de genoemde achterliggende databases en verbindingen daarmee moeten grondig worden getest op verschillende momenten:

1. *Voor aanvang*. Testaanbieders moeten, voordat zij zich op CoronaCheck aan kunnen sluiten, zoals bekend, voldoen aan een serie aansluitvoorwaarden. Het recente datalek bij een commerciële testaanbieder heeft duidelijk gemaakt dat de controle op naleving van de aansluitvoorwaarden, waaronder een pen-test, voor aanvang niet voldoende is geweest.[2] De Begeleidingscommissie adviseert om controle op naleving van de aansluitvoorwaarden voor aanvang aan te scherpen en grondig te controleren of informatiebeveiligingsmaatregelen op het vereiste niveau zijn;

2. *Controle na aanvang*: Recent kon bij een commerciële testaanbieder een datalek optreden dat – zo stelt de minister in zijn brief aan de Tweede Kamer - bij grondige controle vastgesteld zou zijn. In dit specifieke geval had nog geen her-controle na aanvang plaatsgevonden. De begeleidingscommissie adviseert om de controle na aanvang sneller – in de eerste week na aanvang – te doen plaatsvinden;

3. *Periodieke controle*: Dit kan ingericht worden middels het doorlopend blijven scannen en monitoren van de aangesloten partijen en de daarbij gebruikte verbindingen tussen de app en de databases (Systems-to-Systems). De commissie adviseert, mede naar aanleiding van

[1] Advies 19, Begeleidingscommissie DOBC: “Europees test- en vaccinatiepaspoort” (26 april 2021)
Advies 22, Begeleidingscommissie DOBC: “CoronaCheck” (9 juni 2021)

[2] Zie de brief van de minister aan de Tweede Kamer, https://www.rijksoverheid.nl/onderwerpen/coronavirus-covid-19/documenten/kamerstukken/2021/07/18/kamerbrief-over-incident-testcoronanu-bv

het recente datalek, om het monitoringsproces nader aan te scherpen, de periode tussen de scans na aansluiting zo kort mogelijk te houden en deze in opdracht van het ministerie van Volksgezondheid, Welzijn en Sport door een onafhankelijke derde partij uit te laten voeren. Dit alles om mogelijk volgende incidenten te voorkomen.

De volgende aspecten zouden hierbij in ieder geval moeten worden meegenomen:

- Informatieveiligheid van desbetreffende partijen;
- Het voldoen aan de AVG, met name wat betreft de punten:[3]
  - Informatieplicht: in de privacyverklaring moeten aspecten als het uitoefenen van de rechten van de betrokkenen zijn opgenomen;
  - Recht op inzage (kunnen mensen die getest zijn via de website van de aanbieder hun persoonsgegevens inzien, alsmede hun testresultaat) – en dit op een goed beveiligde wijze;
- Er moet per aanbieder gecheckt worden voor welk doel gegevens verzameld worden, hoe deze worden bewaard en wat de bewaartermijnen hiervoor zijn;
- Tot slot moet ook over de tijd heen ge-audit blijven worden of partijen nog steeds voldoen aan de aansluitvoorwaarden die gesteld zijn.

(2) Gebruik van CoronaCheck

De commissie heeft een aantal situaties geconstateerd waarin nog geen optimale gebruikerservaring is met de CoronaCheck app. Het betreft hierbij bijvoorbeeld mensen die bij het inloggen met DigiD nog steeds onterecht een “helaas u moet opnieuw inloggen” scherm te zien krijgen omdat er langer dan 15 minuten geen activiteit was in het scherm. Het handelingsperspectief dat hierbij gegeven wordt geeft echter niet het gewenste resultaat en zorgt er in de ergste gevallen voor dat geen QR-code aangemaakt kan worden.

In navolging hierop wil de commissie adviseren dat in de app duidelijker aangegeven wordt waar burgers terecht kunnen met hun vragen en problemen. Kanalen zoals de veelgestelde vragen op zowel www.coronacheck.nl als de website van de Rijksoverheid, maar ook de (telefonische) helpdesk moeten voor de gebruikers te allen tijde goed zichtbaar en toegankelijk zijn in de app. Dit om onduidelijkheden tegen te gaan en gebruik van de app te blijven stimuleren.

De commissie spreekt ten slotte haar zorg uit over de focus in de keten op het verkrijgen van een “groene vink” ofwel genereren van een QR-code in de CoronaCheck app om weer vaker deel te kunnen nemen in de opengaande samenleving. Dit terwijl er anderzijds nog niet altijd voldoende hulpmiddelen zijn om gebruikers te ondersteunen als dat hen niet lukt. Technische problemen of onduidelijkheden tezamen met een gedeeltelijk toegankelijke app[4] kunnen namelijk (on)bedoeld leiden tot onveilig, ongewenst of afhaak gedrag wat ook kan resulteren in bijvoorbeeld uitsluiting van bepaalde groepen Nederlandse burgers. Denk hierbij bijvoorbeeld aan ouderen, maar ook laaggeletterden en mensen met een beperking. Potentiële effecten hiervan kunnen zijn dat gebruikers nog kwetsbaarder worden, of dat het juist opportunistisch gedrag uitlokt waarbij de focus

[3] In het geval een testaanbieder nog geen inzage aanbiedt en dus in gebreke is w.b.t. AVG, en om dit te repareren nieuwe functionaliteit bouwt, dient deze voordat die aan klanten ter beschikking wordt gesteld, deze middels pentests getest te worden om te verifiëren dat de nieuwe functionaliteit op een goed beveiligde wijze tot stand is gekomen.

[4] De Toegankelijkheidsverklaring van CoronaCheck beschrijft dat de status van de toegankelijkheid van de app in juni 2021 “B: voldoet gedeeltelijk” was. https://www.toegankelijkheidsverklaring.nl/register/4230

van mensen niet zozeer ligt op het voorkomen van besmettingen, maar vooral om zo snel en eenvoudig mogelijk een “groene vink” te verkrijgen.

(3) Inladen van papieren QR-code in CoronaCheck

Sinds 1 juli is ook een webportaal beschikbaar voor alle vaccinatiezetters om op deze manier voor burgers van wie gegevens niet (correct) door CoronaCheck gevonden worden alsnog een Digitaal Corona Certificaat (DCC) te kunnen genereren. Ook voor dit portaal adviseert de commissie om beveiligingsmaatregelen te hanteren zoals eveneens voor CoronaCheck het geval is. Dit ook in het kader van dat een toekomstige release van de app het mogelijk moet maken om deze uitgegeven papieren vaccinatiebewijzen in te laden in CoronaCheck.