Advies 16: Veiligheid & privacy van Covid-19 test en- vaccinatie data

Begeleidingscommissie Digitale Ondersteuning Bestrijding Covid-19

8 februari 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. Deze begeleidingscommissie brengt naast gevraagde adviezen ook ongevraagde adviezen uit.

De Begeleidingscommissie constateert dat Covid-19 leidt tot een exponentiële data-groei, zowel wat betreft de uitslagen van SARS-CoV-2 testen (PCR- en snel-testen), de zeer privacygevoelige contactgegevens verzameld voor het bron- en contactonderzoek (BCO), en de registratie van COVID-19 vaccinaties. Begin december heeft de commissie de GGD'en rechtstreeks geadviseerd met betrekking tot betere afscherming van geregistreerde SARS-CoV-2 testresultaten in de huidige registratiesystemen voor GGD medewerkers. Onderstaand advies is hierop een aanvulling en thans ook gericht aan de minister**: de commissie adviseert een *sense of urgency* te creëren en een cultuuromslag te bewerkstelligen. Expliciet adviseert de commissie een veiligheid- en privacy-inventarisatie bij alle huidige en nieuwe SARS-CoV-2 en Covid-19 gerelateerde data-knooppunten/registratiesystemen, en een verhoging van het veiligheid & privacy bewustzijn zowel bij verantwoordelijke beheerders van deze data-knooppunten/registratiesystemen als bij degenen die toegang tot deze data hebben. Daarnaast adviseert de commissie een publieke campagne op te starten die de huidige problemen en oplossingen beschrijft, en zodra deze datasystemen daadwerkelijk weer privacy-proof zijn dit kenbaar te maken opdat het vertrouwen van de Nederlandse burger kan worden (her)wonnen.** De commissie is zich er terdege van bewust dat de genoemde data-registratiesystemen thans niet direct onder de formele verwerkings-verantwoordelijkheid van VWS vallen. Echter, VWS fungeert wel als opdrachtgever en/of financier en heeft een verantwoordelijkheid voor het gehele coronabeleid, waarvan goede data-security en -privacy een kritische randvoorwaarde is. Gezien het urgente belang adviseert de commissie VWS om alles te doen om snel de data-security en -privacy in deze data-knooppunten/registratiesystemen te verhogen zodat ze weerbaar zijn voor hoge dreigingsniveaus. In het uiterste geval zou wat betreft het databeheer in de GGD koepel, zelfs overwogen moeten worden VWS (tijdelijk) eindverantwoordelijk te maken middels te initiëren noodwetgeving.

(1) Een cultuur van SARS-2-CoV en Covid-19 gerelateerde data-minimalisatie, -privacy en -veiligheid.

De Begeleidingscommissie pleit actief voor data-minimalisatie en privacy-by-default in de strijd tegen Covid-19[1]. Dit is een rode draad geweest bij de ontwikkeling van CoronaMelder en de commissie benadrukt dat deze principes ook op bestaande data-knooppunten/registratiesystemen en andere digitale innovaties t.b.v. de bestrijding van Covid-19 uitgedragen moeten worden.

De begeleidingscommissie heeft op 3 december met de GGD overlegd over de afscherming van NAW gegevens van SARS-CoV-2 geteste personen. Op 9 december mondde dit uit in een praktisch advies rechtstreeks aan de GGD[2]. De kernpunten waren: NAW gegevens van geteste personen uitsluitend toegankelijk maken voor de dossierhouder, additionele beveiliging van HPZone (die door Covid-19 meer dan exponentieel is gegroeid) en brede veiligheidsscans alsook training gericht op afscherming

[1] o.a. Advies 1: Programma van Eisen CoronaMelder

[22] Advies afscherming NAW gegevens geteste Nederlanders (TechTegenCorona).

van Covid-19 gerelateerde gegevens. Hierbij is ook een aanbod gedaan om menskracht en expertise beschikbaar te stellen ten behoeve van het concretiseren van verbeterde data afscherming.

De commissie is zich bewust van de complexe bestuurlijke inbedding van en verantwoordelijkheden over de GGD'en, maar beoogt nu een *sense of urgency* te creëren op dit thema. Versnippering van verantwoordelijkheid voor de diverse data-knooppunten en -registratiesystemen kan het voeren van de noodzakelijke strakke regie belemmeren. De commissie adviseert de minister om de regie te nemen en in het uiterste geval te overwegen om, in ieder geval tijdelijk, de verantwoordelijkheid wat betreft de privacy en veiligheid van deze COVID-19 gerelateerde test- en vaccinatieregistratiesystemen en dataknooppunten centraal te beleggen op het niveau van het ministerie van VWS. De commissie realiseert zich dat daarvoor een wettelijke basis gecreëerd zal moeten worden in een noodwet. In aanvulling daarop is essentieel dat een veiligheid & privacy cultuur wordt bevorderd bij de beheerders van COVID-19 data-knooppunten/registratiesystemen bij allen die toegang hebben tot dergelijke data. Onderdeel van die cultuur is bereidheid tot het bieden van transparantie en aanvaarden van hulp van deskundigen.

Tijdens deze Covid-19 pandemie zijn en zullen er vele data-knooppunten/registratiesystemen in Nederland ontstaan, o.a. bij de GGD'en en het RIVM. Belangrijk hierbij is ook de wettelijke bewaartermijn van deze data. Artsen hebben vanuit de Wet publieke gezondheid (Wpg) een meldplicht aan de GGD, waar een bewaartermijn van zes jaar geldt. De commissie adviseert te overwegen of, wat betreft CoronIT, HPZone en het BCO Portaal, de verwerkingsverantwoordelijke iedere dag alle gegevens ouder dan drie weken kan verwijderen uit de systemen waartoe GGD-medewerkers toegang hebben voor het inplannen van testen en het BCO. Deze data zou in de visie van de commissie vervolgens in gepseudonimiseerde vorm opgeslagen kunnen worden in data-warehouses, waarna nadere analyses ten behoeve van de volksgezondheid kunnen worden uitgevoerd. Alleen een selecte groep daartoe geautoriseerde personen dient dan voor dergelijke analysedoeleinden toegang tot die gegevens te krijgen. Voor zowel de datawarehouses als voor de operationele systemen die toegankelijk moeten zijn voor GGD-medewerkers, geldt dat deze conform de AVG streng beveiligd moeten zijn.

Op dit moment worden zowel de positieve als negatieve SARS-CoV-2 testuitslagen geregistreerd en bewaard. Voor duiding en wetenschappelijk onderzoek is dit van cruciaal belang, maar de blijvende koppeling van al deze negatieve uitslagen aan tot individuen herleidbare data is nog niet goed onderbouwd, waarbij het nog onduidelijk is welke bewaartermijn aangehouden wordt of moet worden: 6 jaar conform de Wet publieke gezondheid of 20 jaar conform de Wet op de geneeskundige behandelingsovereenkomst. De commissie adviseert dat hier een zorgvuldig, goed onderbouwd besluit over wordt genomen en adviseert de minister om ook op dit punt de regie te nemen.

De minister heeft terecht forse financiële middelen vrijgemaakt voor het bron- en contactonderzoek en de Covid-19 vaccinatie. De commissie pleit om expliciet veilig- en privacy vriendelijk databeheer te koppelen aan deze opdrachten, met als resultaat een slagvaardige pandemiebestrijding met een cultuuromslag naar data-minimalisatie, privacy en veiligheid.

(2) Audits op nieuwe SARS-CoV-2 en COVID-19 gerelateerde data-knooppunten/registratiesystemen.

Wij bevelen de minister aan om de verantwoordelijke organisaties op te dragen de komende drie weken externe security, alsook organisatie audits te laten uitvoeren bij de grootste data-knooppunten/registratiesystemen, zoals bijvoorbeeld CoronIT, HPzone, HPzone Lite, Osiris, CIMS, Lareb, het in aanbouw zijnde nieuwe BCO Portaal, alsook bij commerciële SARS-CoV-2 testbedrijven welke met de (semi-) overheid samenwerken, met als doel:

- de data-vergaring en de dataopslag in kaart te brengen en waar mogelijk pseudonimisering toe te passen en data-warehouses op te zetten (zie ook boven).
- de veiligheid en privacy van de systemen alsook de onderlinge verbindingen door te lichten. Naar mening van de commissie dienen deze data-knooppunten/registratiesystemen tot op het hoogst mogelijke niveau beveiligd te zijn. Hierbij is het van belang om te analyseren in hoeverre de toegang van medewerkers tot data geminimaliseerd wordt. Ook is het van belang dat medewerkers niet via een omweg toegang krijgen tot gegevens die niet noodzakelijk zijn. Daar waar toegang nodig is, er expliciet gelogd en gecontroleerd wordt, en waar nodig verbeteringen worden aangebracht. Gestreefd moet worden naar systemen die weerbaar zijn voor hoge dreigingsniveaus.

De commissie vraagt hierbij nadrukkelijk aandacht voor CIMS. Dit wordt de facto een database met bijna de omvang van de gehele Nederlandse bevolking. Het is niet alleen van groot belang om continu te streven naar data-minimalisatie, privacy en beveiliging, het is tevens cruciaal dat burgers worden geïnformeerd wát er met hun data in CIMS gebeurt en/of data wordt gedeeld - en zo ja met wie.

De commissie is van mening dat het essentieel is dat de resultaten van audits niet alleen voor de opdracht-gevende partij (de verwerkingsverantwoordelijke) beschikbaar komen, maar ook voor VWS. Een voorstel kan zijn om de opdracht tot deze audits alsook de financiering vanuit het ministerie te geven en op te zetten, uiteraard met volledige instemming hiervoor van de systeemeigenaar.

(3) Herstel van vertrouwen.

De commissie vreest dat het recente datalek bij de GGD systemen kan leiden tot een afname in test- en wellicht zelfs vaccinatiebereidheid. De exacte omvang van het datalek noch de afname in het vertrouwen kunnen op dit moment niet concreet worden vastgesteld. Recente data lijken aan te tonen dat het aantal afgenomen testen na de bekendwording van het datalek daalt, maar dit is uiteraard moeilijk causaal te relateren aan elkaar. Het effect kan echter snel ongewenste vormen aannemen. Om deze reden adviseert de commissie aan de minister het volgende:

- informeer middels een grootschalige campagne het publiek over de risico's van identiteitsdiefstal. Geef voorbeelden wat er mis kan gaan en geef tips waar op te letten om fraude sneller op te sporen. Daarnaast moet worden gecommuniceerd en uitgelegd dat alles op alles is gezet de systemen te vernieuwen en veilig te maken, en hoe dat geborgd wordt. Zodra de systemen weer voldoen aan de eisen die men daaraan mag stellen, dient dit alles zo snel en helder mogelijk gecommuniceerd te worden.

De commissie adviseert de minister verder om met grote urgentie de volgende verwachtingen te communiceren aan de GGD koepel (GHOR):

- geef het publiek duidelijkheid en inzicht in de stappen die zijn en worden genomen, inclusief de aanbevolen security audits, de uitkomsten en de acties daarop.
- voldoe aan de plicht conform de AVG om alle personen wiens persoonlijke data gestolen zijn door de datalekken uit HPZone en CoronIT – voor zover dit te achterhalen is – te informeren en hulp te bieden als misbruik gemaakt wordt van de gelekte data.
- voldoe aan de plicht conform de AVG om van degenen die het verzoeken, hun persoonlijke data uit bepaalde systemen te verwijderen.