Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

27 529 Informatie- en Communicatietechnologie (ICT) in de Zorg

Nr. 235

BRIEF VAN DE MINISTER VAN VOLKSGEZONDHEID, WELZIJN EN SPORT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 2 februari 2021

Mensen moeten te allen tijde kunnen vertrouwen dat medische gegevens veilig worden gedeeld en bewaard, juist vanwege het privacygevoelige karakter van deze gegevens. Sinds 24 januari zijn er meerdere berichten verschenen over mogelijke datadiefstal bij de GGD'en. Een journalist van RTL heeft bekend gemaakt dat mensen die voor de GGD'en werken datasets met persoonsgegevens uit GGD-systeem HPZone online te koop hebben aangeboden, en persoonsgegevens van individuele personen uit CoronIT te koop aanbieden. Ik betreur dat dit heeft kunnen plaatsvinden. Dit heeft tot maatschappelijke onrust geleid, is zeer ernstig voor de mogelijke slachtoffers en raakt ook alle duizenden medewerkers van de GGD'en die te goeder trouw hun werk doen. Handelen in persoonsgegevens is een misdrijf. De verschillende waarborgen die er al zijn ten behoeve van de omgang met gegevens hebben deze datadiefstal niet kunnen voorkomen.

In deze brief ga ik in op de betreffende ICT-systemen, de rol- en taakverdeling tussen de GGD'en, het Ministerie van VWS en andere betrokken partijen, wet- en regelgeving rondom de verwerking van (medische) persoonsgegevens en blik ik terug op wat er de afgelopen maanden is gebeurd in relatie tot de digitale ondersteuning bij de GGD'en en de veiligheid daarvan, om ten slotte te komen bij de conclusies en te zetten stappen.

Vooraf het volgende: het gaat om gegevens die de GGD'en verwerken in het kader van het testen op het coronavirus en ten behoeve van de infectieziektebestrijding zoals het bron- en contactonderzoek, outbreakmanagement, clusterdetectie en surveillance (zowel landelijk als regionaal). De gegevens worden verwerkt in twee systemen. Allereerst CoronIT waarin testafspraken worden gemaakt en uitslagen teruggekoppeld aan mensen die getest zijn. Het gesignaleerde probleem is dat medewerkers

kst-27529-235
ISSN 0921 - 7371
's-Gravenhage 2021

onrechtmatig persoonsgegevens op hebben kunnen zoeken in dossiers. Uiteraard zijn er bestaande maatregelen zoals het ondergaan van een privacytraining, het tekenen van een geheimhoudingsverklaring, het verplicht stellen van een VOG en het loggen van zoekopdrachten met een steekproefsgewijze controle. Dit bleek niet voldoende. GGD GHOR Nederland heeft besloten dat op korte termijn geautomatiseerde controle mogelijk wordt.
Het andere systeem is HPZone/HPZone Lite. Hier krijgen medewerkers voor het bron- en contactonderzoek toegang tot de gegevens van de GGD-regio waarvoor zij aan het werk gaan. Dit systeem bestond de mogelijkheid om grote databestanden te exporteren. GGD GHOR Nederland heeft aangegeven zo snel mogelijk het gebruik van HPZone te beperken tot een kleine groep specialisten in de infectieziektebestrijding ten behoeve van de surveillance en het maken van analyses om zicht te houden op clusters/uitbraken. Voor het overige gebruik wil zij ten behoeve van de COVID-19 bestrijding zo snel mogelijk van HPZone Lite overstappen op een nieuwe voorziening.

Uit het feitenrelaas -verderop in deze brief- blijkt dat er vanaf het begin van de coronacrisis is gestuurd op het zo snel mogelijk in de lucht krijgen van ICT-systemen die de bestrijding van het virus konden ondersteunen. Daarbij lag de focus primair op de functionaliteit van het systeem: doet het wat we nodig hebben? Daarnaast zijn voortdurend verbeteringen aangebracht om de functionaliteit (o.a. opschaling, meten van doorlooptijden), de bedrijfscontinuïteit (voorkomen van storingen) en gebruikersvriendelijkheid (online testafspraak maken, zelf contacten doorgeven) te verbeteren. Daarbij was steeds ook aandacht voor privacy en dataveiligheid, maar naar nu blijkt onvoldoende.

Hoewel ik begrip heb voor de omstandigheden waarin vooral aandacht was voor de noodzaak dat de systemen zouden werken, is mijn conclusie dat verbeteringen inzake privacy en dataveiligheid en ook andere aspecten sneller moeten worden gerealiseerd en dat strakker op het proces moet worden gestuurd. Daarom onderneem ik in elk geval de volgende vier acties:

1. *Korte termijnacties*. Ik heb als opdrachtgever GGD GHOR Nederland en de GGD'en gevraagd alle maatregelen te treffen die op korte termijn nodig en mogelijk zijn, zoals onder andere:
   - Het gebruik van HPZone zal beperkt worden tot een selecte groep specialisten in de infectieziektebestrijding (IZB-artsen en -verpleegkundigen). Voor het overige gebruik ten behoeve van de COVID-19 bestrijding zal zo snel mogelijk van HPZone Lite overgestapt worden op een nieuwe voorziening die bewijsbaar zal voldoen aan alle standaarden en vereisten inzake privacy en dataveiligheid. Vanzelfsprekend dienen de noodzakelijke functionaliteiten voor COVID-19-bestrijding in die nieuwe voorziening aanwezig te zijn, zodat de regionale en landelijke surveillance zonder onderbreking en tijdig uitgevoerd wordt, waarmee zicht en inzicht op het virus en de bestrijding gewaarborgd blijft. Ik kom hiermee ook tegemoet aan de nadrukkelijke wens van het OMT.
   - De print- en exportfunctie van HPZone (Lite) is reeds uitgeschakeld. Ook in CoronIT is de printfunctie uitgeschakeld of slechts toegankelijk voor een selecte groep specialisten.
   - De toegang en zoekmogelijkheden worden deze week nog beperkt.
   - Er zijn sinds 24 januari gespecialiseerde interne en externe teams dagelijks bezig met het herkennen van verdachte patronen en het opvolgen van verdacht gedrag. Dit blijven zij doen tot het moment dat het systeem geautomatiseerd is, waardoor de pakkans aanzienlijk is vergroot.

- De systemen worden nu door externe IT-deskundigen verder doorgelicht.
- De VOG administratie wordt verder op orde gebracht. De volledige administratie is zo snel als mogelijk – rekening houdend met de doorlooptijden voor de VOG-aanvraag – medio maart op orde.
- Er loopt een intern forensisch onderzoek naar dit misbruik van persoonsgegevens.

2. *Expertise*. De voorzitter van GGD GHOR Nederland heeft mij gevraagd of ik expertise kan leveren om ondersteuning te bieden bij de uitwerking van de te nemen maatregelen en de implementatie daarvan. Deze steun heb ik direct toegezegd. Ik verwacht komende week een eerste kernteam samengesteld te hebben waarin tenminste kennis aanwezig is van privacy en informatiebeveiliging. GGD GHOR Nederland levert de inhoudelijke expertise in dit kernteam.
3. *Strakker sturen*. Er moet door GGD GHOR Nederland en de GGD'en een versnelling plaatsvinden op het uitvoeren van de aanbevelingen die in eerdere onderzoeken, zoals de risicoanalyse, waarover ik uw Kamer heb geïnformeerd op 24 december jl., zijn gedaan. De GGD verwacht dat in maart 2021 alle op korte termijn te realiseren maatregelen zijn getroffen. De stuurgroep Landelijke Coördinatiestructuur Testcapaciteit (LCT) adviseert mij op basis van de wekelijkse rapportage van de regiegroep Digitale Ondersteuning van de Test- en Traceerketen (DOTT). GGD GHOR Nederland rapporteert over de voortgang van het realiseren van de verbeteringen aan de regiegroep DOTT die wekelijks bijeenkomt. De regiegroep wordt onder meer geadviseerd door het Nationaal Cyber Security Centre (NCSC), de chief information officer (CIO) van de rijksoverheid, de informatiebeveiligingsorganisatie voor de zorg Z-CERT en andere experts.
4. *Externe audit*. GGD GHOR Nederland en ik geven samen opdracht tot een externe audit van beide systemen over 6 weken. Deze audit gaat na of de adviezen zijn opgevolgd, in hoeverre de aangekondigde maatregelen daadwerkelijk zijn getroffen en wat de resterende risico's zijn.

Wijzigingen worden zodanig doorgevoerd dat de COVID-19-bestrijding zonder onderbreking doorgang kan vinden. Uitvoering van test-, traceer- en vaccineerprocessen alsmede de landelijke en regionale surveillance en (cluster)analyses zijn randvoorwaardelijk voor het spoedig achter ons laten van de pandemie. Een vertegenwoordiging van inhoudelijke GGD en RIVM professionals adviseert hierover en stelt vast of (nieuwe) voorzieningen gebruiksklaar zijn.

Communicatie (potentiële) slachtoffers

Als dit misbruik van persoonsgegevens heeft kunnen plaatsvinden, is dat in de eerste plaats ernstig voor de mensen die hier slachtoffer van zijn geworden. GGD GHOR meldt dat zij sinds 29 januari 2021 actief zijn gaan communiceren over de achtergronden van de datadiefstal, de maatregelen die genomen zijn en genomen worden. Inmiddels is een telefoonnummer geopend waar burgers 7 dagen per week van 9 tot 21 uur terecht kunnen met hun vragen. GGD GHOR Nederland heeft mij gemeld dat wanneer bekend is wie slachtoffer is geworden van datadiefstal, de GGD contact met hen zal opnemen.

Vanuit de overheid worden er ook publiekscampagnes ingezet om mensen voor te lichten over bewustwording en het bieden van handelingsperspectief in geval van cybercriminaliteit en online fraude. Meer informatie over deze campagnes is te vinden op www.maakhetzenietteemakkelijk.nl en www.veiliginternetten.nl. Op deze websites is ook

informatie te vinden over wat men zelf kan doen om deze risico's te verkleinen.

Strafrechtelijk onderzoek

Er is ook een strafrechtelijk onderzoek gestart. Het openbaar ministerie heeft naar aanleiding van een melding van mogelijke datadiefstal bij de GGD'en onmiddellijk actie ondernomen door een opsporingsonderzoek te starten en heeft kort na de start van dit onderzoek verschillende verdachten aangehouden en voorgeleid. Daarbij zijn onder meer telefoons in beslag genomen en wordt berichtenverkeer in kaart gebracht. Het stelen van data en het verhandelen ervan is strafbaar. Het openbaar ministerie treedt daar in zulke gevallen adequaat tegen op. Of en zo ja in welke mate in het onderhavige geval data zijn gestolen en/of verhandeld is nog in onderzoek.

Informatievoorziening

Om uw Kamer zo volledig mogelijk te informeren is in een bijlage een eerste feitenrelaas vanuit zowel de GGD'en als mijn ministerie toegevoegd. Gelet op de korte tijd die hiervoor beschikbaar was, kan ik niet uitsluiten dat op een later moment aanvullende informatie beschikbaar komt. Uiteraard zal ik uw Kamer daarover dan informeren.

Inzet van ICT-systemen voor bron- en contactonderzoek en testen

Met de uitbraak van deze pandemie hebben de GGD'en hun capaciteit om te testen en traceren drastisch opgeschaald om uitvoering te kunnen geven aan de ongekende vraag naar testen en bron- en contactonderzoek. Om bron- en contactonderzoek uit te voeren maakten de GGD'en al sinds 2003 gebruik van het IT-systeem HPZone. Bij het begin van de uitbraak van het coronavirus hebben zij besloten dit ook in te zetten voor de bestrijding van deze pandemie. Elk van de GGD'en heeft van dit systeem een eigen implementatie. Toen landelijke opschaling nodig was en een nieuwe groep bron- en contactonderzoekers landelijk ging opereren is in juni aanvullend HPZone Lite toegevoegd. Daarmee kregen de medewerkers van de landelijke schil van bron- en contactonderzoekers toegang tot de noodzakelijke gegevens. HPZone (Lite) bevatte tot voor kort een print- en exportfunctie die beschikbaar was voor veel medewerkers. Deze functie werd voor de opschaling gebruikt voor werkverdeling en epidemiologische analyses van uitbraken (clusteranalyses). De noodzaak tot snelle en massale opschaling heeft geleid tot de situatie waarin deze functie voor veel mensen beschikbaar was.

Testen op het coronavirus op de huidige schaal is voor de GGD'en een nieuwe taak. GGD GHOR Nederland meldt mij dat het niet zo is dat alle medewerkers bij alle gegevens in CoronIT kunnen. Door middel van rollen en hieraan gekoppelde rechten wordt toegang verschaft. Iemand die vaccinatieafspraken maakt, kan wel de testgegevens zien omdat dat nodig kan zijn om te bepalen of een persoon gevaccineerd kan worden. Iemand die een testafspraak maakt, kan een vaccinatieafspraak wel zien, maar niet de overige bijbehorende gegevens. Ik heb aan GGD-GHOR gevraagd nog eens zeer kritisch tegen het licht te houden wat echt nodig is ten aanzien van deze functionaliteit voor het uitvoeren van testen en vaccineren en mij hierover op korte termijn te berichten. Overigens bevatte CoronIT tot voor kort een printfunctie die gebruikt werd bij noodprocedures. Deze functie is uitgezet.

Daarnaast heb ik in de vorige voortgangsbrief aan uw Kamer gemeld dat het centrale informatiesysteem (Covid-19 vaccinatie informatie- en

monitoringssysteem, CIMS) in gebruik is genomen door het RIVM (Kamerstuk 25 295, nr. 874). Het systeem zal gevuld worden vanuit de verschillende decentrale systemen, waaronder dat van de GGD'en. Ik heb aangegeven dat het RIVM een proces heeft ingericht voor het beheer en doorontwikkelen van het landelijk register en het nemen van eventuele aanvullend benodigde informatiebeveiligingsmaatregelen. Dit laatste – de informatieveiligheid – is extra actueel geworden naar aanleiding van de recente gebeurtenissen rondom de beveiliging van het GGD-testsysteem. Aan veilige koppelingen met de decentrale systemen is uitgebreid aandacht besteed, zoals ook in eerdere brieven beschreven. Eind december is in het kader van de Data Protection Impact Assessment zeer uitgebreid onderzoek gedaan, door het RIVM zelf en door externen, naar privacy- en informatiebeveiligingsaspecten van CIMS. Naar aanleiding van deze onderzoeken zijn verdere maatregelen genomen om CIMS te beveiligen. Naar aanleiding van de recente gebeurtenissen bij de GGD'en is nog eens een aanvullende risicoanalyse gevraagd. Het RIVM heeft immers de verantwoordelijkheid voor een grote hoeveelheid bijzondere persoonsgegevens van veel Nederlanders. De gevolgen van eventuele gebreken in de bescherming van deze gegevens zouden eveneens groot zijn. Het RIVM geeft aan dat de kans op een inbreuk zoals bij het GGD-systeem gering is. Dit onder meer omdat slechts een beperkt aantal mensen bij de gegevens kan, er geen export- of printfunctie voor eindgebruikers is, en dat de werkzaamheden van eindgebruikers vanuit een gecontroleerde omgeving (kantoor) gebeuren. Alle activiteiten worden gelogd en gecheckt. De komende maanden worden de bestaande detectie- en monitoringcapaciteiten verder verbeterd.

Rol- en taakverdeling en wet- en regelgeving

De rijksoverheid en gemeenten hebben in de Wet publieke gezondheidszorg (Wpg) onderscheiden taken en verantwoordelijkheden. Als Minister van Volksgezondheid, Welzijn en Sport heb ik de wettelijke taak om de kwaliteit en doelmatigheid van de publieke gezondheidszorg te bevorderen en om zorg te dragen voor de instandhouding van de landelijke ondersteuningsstructuur (RIVM).

Gemeenten zijn verplicht een gezondheidsdienst (GGD) in stand te houden aan wie specifieke wettelijke taken zijn toebedeeld. Zij worden voor die taken gefinancierd door de gemeenten. Elke GGD staat onder leiding van een directeur publieke gezondheid (DPG). De DPG'en hebben zich verenigd in de Raad van DPG'en en hun belangen worden behartigd door GGD GHOR Nederland Nederland.

Normaliter draagt het college van burgemeester en wethouders zorg voor de uitvoering van de algemene infectieziektebestrijding, waaronder het nemen van algemene preventieve maatregelen en bron- en contactonderzoek na melding bij de GGD'en. Het uitvoeren van een dergelijk bron- en contactopsporing vindt altijd plaats op grond van de vrijwillige medewerking van de besmette betrokkene (Kamerstuk 31 316, nr. 3, p. 35–36). Ingeval van een epidemie van een infectieziekte behorend tot groep A, zoals het geval is bij het coronavirus, is het de voorzitter van de veiligheidsregio die zorg moet dragen voor de bestrijding van de epidemie. De leiding ligt in dat geval bij mij, als Minister van VWS, en ik kan in dat verband aanwijzingen geven aan de voorzitters van de veiligheidsregio's. Het RIVM, specifiek het Centrum voor Infectieziektebestrijding (CIb), heeft bij landelijke uitbraken de coördinatie van de bestrijding in handen. Het CIb formuleert het bestrijdingsbeleid en geeft advies aan de overheid en de professionals in de praktijk. Het zorgt voor heldere en betrouwbare communicatie naar publiek en professionals

onder andere door het opstellen van inhoudelijke richtlijnen over de uitvoering van taken inzake de infectieziektebestrijding.

De Wet publieke gezondheid (Wpg) regelt onder meer de melding van infectieziekten aan de GGD'en en de daarbij te verstrekken persoonsgegevens en de bewaartermijn van die gegevens. Een melding aan de GGD van een arts bij de vaststelling van een infectie door het coronavirus (groep A) dient onder andere te bestaan uit specifieke persoonsgegevens, zoals naam, adres, geslacht, geboortedatum, burgerservicenummer, verblijfplaats van de betrokken persoon en een beschrijving van het ziektebeeld, de eerste ziektedag, de vaccinatietoestand, de vermoedelijke infectiebron, de datum van vermoeden of vaststelling van de infectie en de wijze van vaststelling van de infectieziekte. Een arts die een onderzoek bij een laboratorium aanvraagt, stuurt de naam, geboortedatum en het burgerservicenummer van de betrokken persoon mee. De GGD is gehouden de persoonsgegevens op te nemen in een registratie en deze gegevens die worden gebruikt in het kader van bron- en contactonderzoek hoogstens 5 jaar te bewaren.

Bij de uitbraak van de covid-19 pandemie in Nederland, heb ik de GGD'en gevraagd om aanvullend op, maar passend bij hun reguliere, wettelijke taken inzake de infectieziektebestrijding, het testen (en traceren) van mensen met klachten die passen bij covid-19 uit te voeren. Het testen op covid-19 is geen wettelijke taak van de GGD'en, maar is wel een taak die logischerwijs bij de GGD'en belegd is. Het afnemen van diagnostiek is bijvoorbeeld wel een standaard onderdeel van het generieke draaiboek voor grootschalige infectieziektebestrijding van de Landelijke Coördinatie Infectieziektebestrijding (LCI). De GGD'en zijn daarom de meest aangewezen organisaties om deze noodzakelijke taak uit te voeren, ondanks dat zij niet voorbereid waren op een taak van deze omvang.

De GGD treedt, als het gaat om testen, op als zorgverlener en heeft daardoor een behandelovereenkomst met de betrokken burger. Die overeenkomst is de basis om persoonsgegevens te verwerken. In dit kader heeft de GGD als zorgaanbieder de verplichting het Burgerservicenummer (BSN) te registreren van betrokkene en ook een medisch dossier bij te houden op grond van de Wet op de Geneeskundige behandelingsovereenkomst (Wgbo), waarin op basis van BSN geregistreerd moet worden. De Wgbo bepaalt onder meer dat medische dossiers twintig jaar moeten worden bewaard (te rekenen vanaf het tijdstip waarop de laatste wijziging in het dossier heeft plaatsgevonden).

De afgelopen weken werd ter discussie gesteld waarom de GGD gegevens bewaart. Het bewaren van persoonsgegevens is juridisch noodzakelijk en tevens praktisch nuttig. De bewaartermijnen van zowel de Wet publieke gezondheid als de Wgbo staan verwijderen van persoonsgegevens niet zonder meer toe. De beveiliging van medische dossiers, waaronder de procedures om dossiers in te kunnen zien, is de verantwoordelijkheid van de zorgaanbieder zelf en de regels zijn streng en duidelijk. Een zorgaanbieder dient van iedere inzage logging te bewaren en deze periodiek te controleren op eventueel misbruik. Dat heeft de GGD overigens ook gedaan. De GGD meldt mij dat vanwege de structurele steekproefsgewijze controle van logbestanden op onrechtmatige toegang de afgelopen tijd circa 30 mensen zijn ontslagen. De Inspectie Gezondheidszorg en Jeugd (IGJ) houdt toezicht op en handhaaft deze wettelijke verplichtingen vanuit de borging van de kwaliteit van zorg en de Autoriteit Persoonsgegevens (AP) houdt toezicht op dergelijk misbruik van persoonsgegevens via Algemene Verordening Gegevensbescherming (AVG).

GGD GHOR Nederland heeft mij gemeld dat volledige persoonsgegevens ook praktisch nodig zijn om het werk van de virusbestrijding te kunnen uitvoeren. Allereerst zodat zeker is dat een test- of vaccinatie-afspraak met de juiste persoon wordt gemaakt. Het BSN is noodzakelijk voor de controle van de identiteit, en is daarnaast belangrijk zodat in CoronIT automatisch de juiste persoonsgegevens geregistreerd worden in plaats van dat alle persoonsgegevens handmatig ingevoerd moeten worden (met het risico op administratieve fouten). Daarnaast is het BSN gekoppeld aan DigiD, wat het mogelijk maakt om de uitslag online in te zien. Het woonadres is nodig, zodat de GGD'en de uitslag ook per brief kunnen toesturen indien er onverhoopt een verkeerd telefoonnummer is geregistreerd en daardoor iemand de uitslag niet heeft kunnen ontvangen.
De gegevens zoals geregistreerd in CoronIT zijn opgenomen in de privacyverklaring CoronIT. Ook de gegevens zoals geregistreerd in HPZone zijn terug te vinden in de privacyverklaring van bron- en contactonderzoek in het kader van COVID-19.

Zorgprofessionals moeten in het algemeen in het kader van hun werk kunnen beschikken over de juiste informatie, op het juiste moment en op de juiste plaats. De Minister voor Medische Zorg en Sport onderzoekt op verzoek van het lid Raemakers van uw Kamer of niet in meer situaties kan worden uitgegaan van het Estlandse vertrouwensmodel[1] waarin medewerkers van zorgaanbieders op basis van «high trust, high penalty» worden vertrouwd – tot het tegendeel bewezen is – in het goed omgaan met de informatie waarover ze kunnen beschikken.

Verzoek van uw Kamer

In de komende passages zal ik ingaan op sleutelmomenten in de tijd. Een uitgebreid overzicht van feiten op basis van officiële documenten inzake de communicatie tussen het Ministerie van VWS, de GGD'en en eventueel andere relevante derde partijen over de informatievoorziening van de GGD heb ik bijgevoegd. Onderliggende stukken heb ik uw Kamer inmiddels ook doen toekomen. Ik heb daarin gepoogd zo volledig mogelijk te zijn. Gezien het korte tijdsbestek, kan ik niet uitsluiten dat er nog meer stukken beschikbaar komen die relevant zijn. Zoals gezegd zal ik ook deze stukken dan zo spoedig mogelijk met uw Kamer delen.

Incidenten en risico's

In **mei 2020** werd CoronIT stapsgewijs in gebruik genomen om mogelijk te maken dat alle Nederlanders met klachten passend bij Covid-19 zich konden laten testen per 1 juni 2020. Bij de start van CoronIT zijn door drie partijen testen uitgevoerd op informatieveiligheid en privacy. Na de eerste introductie is er voortdurend verder gewerkt aan het verbeteren van het systeem. Ondanks deze verbeteringen laten verschillende signalen en incidenten in de zomer en het najaar van 2020 zien dat de digitale test- en traceerketen niet optimaal functioneert. De problemen die zich voordeden hadden te maken met de *continuïteit en kwaliteit van gegevens* en met de *beveiliging van systemen*.

Continuïteit en kwaliteit van gegevens.

Op meerdere momenten was er sprake van storingen waardoor besmettingscijfers met vertraging werden weergegeven. Zo werd in de maand juli de eerste storing in de test- en traceerketen gemeld. De oorzaak van de storing leek terug te voeren tot CoronIT. Op **16 juli 2020** heb ik uw

[1] Kamerstuk 27 529, nr. 221

Kamer gemeld dat GGD GHOR Nederland aangaf in te zetten op verdere verbeteringen van het systeem CoronIT[2]. Op **6 augustus** meldde ik uw Kamer dat deze verbeteringen naar verwachting per **1 september** zouden zijn doorgevoerd.[3] Op **17 september** meldde de Inspectie Gezondheidszorg en Jeugd dat zij gaandeweg haar toezichtsonderzoek steeds meer stabiliteit en koppelingen zag ontstaan waardoor de knelpunten op ICT-gebied steeds minder werden. **Eind oktober** zijn er wederom technische storingen in het systeem van de GGD'en. Dit leidt opnieuw tot onvolledigheid in de dagelijkse cijfers. GGD GHOR Nederland heeft hierop maatregelen getroffen om de robuustheid van de infrastructuur van onder andere HPZone en de koppelingen te verbeteren.

Beveiliging van systemen.

Op **16 september** bericht Nieuwsuur dat medewerkers van de GGD inzage hebben in alle persoonsgegevens die ten behoeve van testen en traceren zijn opgeslagen. In **september 2020** heeft de Autoriteit Persoonsgegevens informatie gevraagd over de verwerking en bescherming van persoonsgegevens in het kader van de coronatestlijn; de daarbij betrokken partijen; de daaraan gerelateerde systemen; de waarborgen ter bescherming van de persoonsgegevens; het toegangs- en/of autorisatiebeleid; logging en de gegevensbeschermingseffectbeoordeling. De gevraagde informatie is aan de Autoriteit Persoonsgegevens verstrekt. Op **3 november** bericht het AD dat medewerkers van de GGD zichzelf ongeoorloofd toegang hebben verschaft tot de persoonlijke gegevens van bekende personen die geregistreerd staan in het IT-systeem. In reactie op deze signalen meldt de GGD dat alle callcentermedewerkers bij alle dossiers kunnen omdat ze de informatie van mensen die bellen voor een afspraak moeten kunnen controleren. Ook meldt de GGD dat medewerkers een geheimhoudingsverklaring moeten ondertekenen en dat er scherp gecontroleerd wordt op wie wat doet in het systeem. Daarbij worden er maatregelen genomen als blijkt dat een medewerker de regels overtreedt[4].

Tijdens het mondelinge vragenuur van afgelopen dinsdag 26 januari heb ik gezegd dat de GGD sinds de start van de pandemie «continu het gebruik van de systemen» controleert. Dit heeft ten onrechte bij sommigen de indruk gewekt dat er nu reeds sprake is van een geautomatiseerde controle, terwijl de GGD tot nu toe structureel steekproefsgewijs controleert. Ik heb daarna gezegd dat «die controles ook worden geautomatiseerd, zodat ze volcontinu kunnen worden uitgevoerd», en had daarbij voor de helderheid beter kunnen aangeven dat dit pas in maart gerealiseerd zal zijn. Ik betreur dat hierover misverstanden zijn ontstaan en zet dit in deze brief recht.

Op **17 november** is er een technische briefing voor de Vaste Commissie voor Volksgezondheid, Welzijn en Sport door André van der Zande, voorzitter Landelijke Coördinatiestructuur Testcapaciteit. In de briefing komt ook de verwerking van persoonsgegevens in de test- en traceerketen aan de orde. Door de leden Agema (PVV) en Özturk (DENK) worden vragen gesteld over de veiligheid van gegevens van burgers, zoals Burgerservicenummers, maar ook van lichaamsmateriaal. Op **18 november** wordt over het gebruik van lichaamsmateriaal na het afnemen van een coronatest tevens een motie ingediend door het lid Kuzu (DENK).[5] In mijn stand van zakenbrief van **8 december** heb ik uiteengezet

---

[2] Kamerstuk 25 295, nr. 460.
[3] Kamerstuk 25 295, nr. 469.
[4] Aanhangsel Handelingen II 2020/21, nrs. 825 en 826.
[5] Kamerstuk 25 295, nr. 735.

hoe en waarom deze gegevens van burgers worden opgeslagen en welke regels hieraan verbonden zijn.

Risicoanalyse en Regiegroep DOTT

Naast dat op elk signaal is gehandeld hebben bovengenoemde signalen en incidenten ertoe geleid dat in **november** de Regiegroep Digitale Ondersteuning Test- en Traceerketen (DOTT) wordt ingericht en is besloten door VWS, GGD GHOR Nederland en het RIVM tot het uitvoeren van een gezamenlijke risicoanalyse op «de IT-systemen en gegevensuitwisseling in de test- en traceerketen Covid-19». Deze risicoanalyse moest toezien op de gehele keten. Gelijktijdig besluit GGD GHOR Nederland een eigen analyse te laten uitvoeren op de interne systemen door KPMG. Deze eigen analyse van GGD GHOR Nederland is 20 januari opgeleverd en op 30 januari vertrouwelijk met het Ministerie van VWS gedeeld.

De risicoanalyse die in opdracht van VWS, GGD GHOR Nederland en het RIVM werd uitgevoerd had als doel om te beoordelen of en waar een versteviging, uitbouw en – waar nodig – herontwerp van de onderliggende ICT-infrastructuur verstandig is. De analyse is in zeer korte tijd uitgevoerd aan de hand van interviews en het doornemen van documentatie. Er is geen audit uitgevoerd. Deze rapportage is eind december 2020 opgeleverd. Over de resultaten van de risicoanalyse heb ik uw Kamer bij brief geïnformeerd op **24 december**[6] . In overleg met het Nationaal Cyber Security Center (NCSC) is besloten om het rapport zelf om veiligheidsredenen niet openbaar te maken. De Regieroep DOTT is verantwoordelijk voor de opvolging van deze risicoanalyse. De Regiegroep DOTT is een samenwerking tussen VWS, GGD GHOR Nederland en het RIVM. De regiegroep rapporteert aan de LCT.

Twee belangrijke onderdelen van de analyse waren de *beveiliging van systemen* en de *continuïteit en kwaliteit van gegevens*. Hiervan werden zowel risico's als preventieve en correctieve maatregelen beschreven.

Beveiliging van systemen.

De vraag wie toegang heeft tot systemen waarin persoonsgegevens worden verwerkt, begint bij de screening van medewerkers. Om misbruik van informatie door medewerkers te voorkomen beschrijft de risicoanalyse verschillende voorzorgmaatregelen. Medewerkers moeten voor aanvang van hun werkzaamheden een geheimhoudingsverklaring ondertekenen en het omgaan met vertrouwelijke informatie is een belangrijk onderdeel van het inwerkprogramma. Daarnaast wordt van medewerkers een VOG gevraagd, maar beschrijft de risicoanalyse ook dat zij in afwachting van de VOG mogen starten met werken. Dat laatste is niet ongebruikelijk. De noodzaak om de capaciteit van de test- en traceerketen snel op te schalen was groot en bovendien zaten door de sluiting van onder andere de horeca veel mensen zonder werk thuis. Behalve voorzorgmaatregelen meldt de GGD in de risicoanalyse ook dat zij maatregelen neemt wanneer een medewerker toch de regels overtreedt en ten behoeve daarvan de activiteiten van medewerkers in het systeem controleert door middel van logging. De risicoanalyse beschrijft dat er maatregelen bestaan om ongewenst en verdacht gedrag te detecteren. De kennis van de maatregelen ten aanzien van de toegang tot systemen is opgedaan in interviews en aan de hand van documentatie. Er is bij het opstellen van de analyse geen audit gedaan op bestaan en werking van de maatregelen.

---

[6] Kamerstuk 25 755, nr. 843

In mijn antwoord tijdens het mondelinge vragenuur van vorige week heb ik u gemeld dat «het systeem van de GGD voldoet aan de laatste NEN-norm». Dit klopt strikt genomen ook, maar had ik achteraf gezien duidelijker moeten formuleren. Het software-platform van Topicus waar CoronIT onderdeel van uitmaakt is volledig gecertificeerd. Echter, de organisatie van GGD GHOR Nederland voldoet nog niet aan deze norm. Zij bereidt zich wel voor op certificatie volgens NEN-7510.

Continuïteit en kwaliteit van gegevens.

Storingen in de IT-systemen die leidden tot een vertraging in de cijfers waren een tweede aanleiding voor de risicoanalyse. Daarom is er gekeken naar de continuïteit en de kwaliteit van gegevens. Hierover heb ik in mijn brief van 24 december het volgende aan uw Kamer medegedeeld:

De gegevensuitwisseling is te karakteriseren als een estafette: op verschillende momenten in de tijd worden door individuele ketenpartners gegevens aan elkaar overgedragen. Dit betreft meerdere soorten gegevens, zoals persoonsgegevens, testuitslagen, logistieke en stuurgegevens, alsmede data voor onderzoek en rapportage. Over de manier waarop informatie wordt uitgewisseld zijn tussen de ketenpartners afspraken gemaakt. De risicoanalyse legt enkele kwetsbaarheden bloot, onder meer op het gebied van informatiebeveiliging, IT-continuïteit, datakwaliteit en toekomstbestendigheid. In de kern komt het erop neer dat twee van de drie gebruikte IT-systemen in het verleden zijn gebouwd voor verschillende doeleinden, waardoor systemen onvoldoende op elkaar aansluiten. Hierdoor is het IT-landschap niet optimaal geschikt voor gebruik tijdens een pandemiesituatie. Dit veroorzaakte de afgelopen maanden verschillende storingen.

Naar aanleiding van de incidenten zijn er reeds verbeteringen doorgevoerd en is er een ketenbreed incidentenproces ingericht.

Direct na het bekend worden van de mogelijke handel in persoonsgegevens heb ik met GGD GHOR Nederland afgesproken dat onder mijn verantwoordelijkheid zou worden gestart met een «Red Team». Dit is de naam voor een aanpak om de digitale verdediging van een organisatie en van systemen te testen. Gebleken is dat het team er in is geslaagd om zich toegang te verschaffen tot documenten die niet beschikbaar zouden moeten zijn. Het team continueert zijn werkzaamheden en zodra er meer zicht is op de feiten en de opvolging daarvan zal ik uw Kamer informeren.

Follow up risicoanalyses: verbeterplan

De risicoanalyse heeft tot vier concrete actiepunten geleid, die ik in mijn brief van 24 december aan uw Kamer heb aangekondigd en die nu onder versterkte regie worden opgepakt[7] . Naar aanleiding van de risicoanalyse heeft de voorzitter van de LCT de Regiegroep DOTT opdracht gegeven tot het opstellen van een ketenbreed verbeterplan. Dit verbeterplan zal naar verwachting donderdag 4 februari 2021 ter advies worden voorgelegd aan de LCT. Wanneer de LCT positief besluit te adviseren, zal ik dit verbeterplan aan uw Kamer doen toezenden. Toch heb ik gezien de terechte focus op dit onderwerp de voorzitter gevraagd de uitgangspunten voortijdig met mij te delen.

De voorzitter geeft aan dat het verbeterplan de focus uitdrukkelijk zal leggen bij het op orde brengen van de basis. De doelstelling van dit verbeterplan is het zo snel mogelijk onder controle krijgen van de

[7] Kamerstuk 25 295 nr. 843

oorzaken van de problemen en vervolgens het duurzaam inrichten van de keten voor de toekomst. Het plan adresseert de belangrijkste risico's en zal zijn onder te verdelen in drie hoofdonderwerpen, namelijk (1) het herijken en herinrichten van het ICT-landschap (de techniek), (2) informatiebeveiliging en privacy (de beveiliging en de mens) en (3) informatie-uitwisseling in de keten (de gegevensuitwisseling).

GGD GHOR Nederland werkt naar aanleiding van de interne risicoanalyse door KPMG aan een verbeterde besluitvorming/governance en organisatie-inrichting. Tevens werkt zij aan het aanscherpen van eisen aan leveranciers om die in lijn te brengen met de eisen die gesteld worden door de schaal en dynamiek die de COVID-19 bestrijding stellen. Ook wordt een wijziging in de architectuur van koppelingen tussen de belangrijkste systemen doorgevoerd en wordt het testen van het ICT landschap opgeschaald om voorbereid te zijn op aanvullende taken en belasting.

Conclusie

Verbeteringen inzake privacy en dataveiligheid en ook andere aspecten moeten sneller worden gerealiseerd en er moet strakker op het proces worden gestuurd.

Daarom onderneem ik in elk geval de volgende vier acties:

1. *Korte termijnacties*. Ik heb als opdrachtgever GGD GHOR Nederland en de GGD'en gevraagd alle maatregelen te treffen die op korte termijn nodig en mogelijk zijn.
   - Het gebruik van HPZone zal beperkt worden tot een selecte groep specialisten in de infectieziektebestrijding (IZB-artsen en -verpleegkundigen). Voor het overige gebruik ten behoeve van de COVID-19 bestrijding zal zo snel mogelijk van HPZone Lite overgestapt worden op een nieuwe voorziening die bewijsbaar zal voldoen aan alle standaarden en vereisten inzake privacy en dataveiligheid. Vanzelfsprekend dienen de noodzakelijke functionaliteiten voor COVID-19-bestrijding in die nieuwe voorziening aanwezig te zijn, zodat de regionale en landelijke surveillance zonder onderbreking en tijdig uitgevoerd wordt, waarmee zicht en inzicht op het virus en de bestrijding gewaarborgd blijft. Ik kom hiermee ook tegemoet aan de nadrukkelijke wens van het OMT.
   - GGD GHOR Nederland en de GGD'en hebben afgesproken dat de commissie COVID van de DPG Raad het mandaat heeft om maatregelen rond HP Zone te nemen indien dat verantwoord is. Daarbij heeft de DPG Raad besloten om nader te onderzoeken welke alternatieven het meest gewenst zijn. In dit onderzoek spelen techniek, veiligheid en functionaliteit een rol. GGD Contact, waarover ik uw Kamer eerder informeerde, wordt daarbij meegenomen.
   - De print- en exportfunctie van HPZone (Lite) is reeds uitgeschakeld. Ook in CoronIT is de printfunctie uitgeschakeld of slechts toegankelijk voor een selecte groep specialisten.
   - De toegang en zoekmogelijkheden worden deze week nog beperkt.
   - Er zijn sinds 24 januari gespecialiseerde interne en externe teams dagelijks bezig met het herkennen van verdachte patronen en het opvolgen van verdacht gedrag. Dit blijven zij doen tot het moment dat het systeem geautomatiseerd is, waardoor de pakkans aanzienlijk is vergroot.
   - De systemen worden nu door externe IT-deskundigen verder doorgelicht.
   - De VOG administratie wordt verder op orde gebracht. Na inventarisatie missen circa 150 verklaringen. De volledige administratie is zo

snel als mogelijk – rekening houdend met de doorlooptijden voor de VOG-aanvraag – medio maart op orde.
   – Er loopt een intern forensisch onderzoek naar dit misbruik van persoonsgegevens.
2. *Expertise*. De voorzitter van GGD GHOR Nederland heeft mij gevraagd of ik expertise kan leveren om ondersteuning te bieden bij de uitwerking van de te nemen maatregelen en de implementatie daarvan. Deze steun heb ik direct toegezegd. Ik verwacht komende week een eerste kernteam samengesteld te hebben waarin tenminste kennis aanwezig is van privacy en informatiebeveiliging. GGD GHOR Nederland levert de inhoudelijke expertise in dit kernteam.
3. *Strakker sturen*. Er moet door GGD GHOR Nederland en de GGD'en een versnelling plaatsvinden op het uitvoeren van de aanbevelingen die in eerdere onderzoeken, zoals de risicoanalyse, waarover ik uw Kamer heb geïnformeerd op 24 december jl., zijn gedaan. De GGD verwacht dat in maart 2021 alle op korte termijn te realiseren maatregelen zijn getroffen. De stuurgroep Landelijke Coördinatiestructuur Testcapaciteit (LCT) adviseert mij op basis van de wekelijkse rapportage van de regiegroep Digitale Ondersteuning van de Test- en Traceerketen (DOTT). GGD GHOR Nederland rapporteert over de voortgang van het realiseren van de verbeteringen aan de regiegroep DOTT die wekelijks bijeenkomt. De regiegroep wordt onder meer geadviseerd door het Nationaal Cyber Security Centre (NCSC), de chief information officer (CIO) van de rijksoverheid, de informatiebeveiligingsorganisatie voor de zorg Z-CERT en andere experts.
4. *Externe audit*. GGD GHOR Nederland Nederland en ik geven samen opdracht tot een externe audit over 6 weken. Deze audit gaat na of de adviezen zijn opgevolgd, in hoeverre de aangekondigde maatregelen daadwerkelijk zijn getroffen en wat de resterende risico's zijn.

Wijzigingen in het ICT landschap worden zodanig doorgevoerd dat de COVID-19-bestrijding zonder onderbreking doorgang kan vinden. Uitvoering van test-, traceer- en vaccineerprocessen alsmede de landelijke en regionale surveillance en (cluster)analyses zijn randvoorwaardelijk voor het spoedig achter ons laten van de pandemie. Een vertegenwoordiging van inhoudelijke GGD en RIVM professionals adviseren hierover en stellen vast of (nieuwe) voorzieningen gebruiksklaar zijn.

De Minister van Volksgezondheid, Welzijn en Sport,
H.M. de Jonge