2021D03895

INBRENG VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

In de vaste commissie voor Volksgezondheid, Welzijn en Sport bestond bij enkele fracties behoefte een aantal vragen en opmerkingen voor te leggen aan de Minister van Volksgezondheid, Welzijn en Sport betreffende het datalek bij de coronasystemen van de GGD[1].

De voorzitter van de commissie,
Lodders

De adjunct-griffier van de commissie,
Heller

[1] RTL Nieuws, 25 januari 2021, «Illegale handel in privégegevens miljoenen Nederlanders uit coronasystemen GGD» (https://www.rtlnieuws.nl/nieuws/nederland/artikel/5210644/handel-gegevens-nederlanders-ggd-systemen-database-coronit-hpzone)

Inhoudsopgave **blz.**

I. Vragen en opmerkingen vanuit de fracties

Vragen en opmerkingen van de VVD-fractie

De leden van de VVD-fractie hebben met zorgen kennisgenomen van het bericht over het datalek bij de coronasystemen van de Gemeentelijke Gezondheidsdienst (GGD). Genoemde leden vinden dat te allen tijde zorgvuldig en vertrouwelijk moet worden omgegaan met grote hoeveelheden persoonsgegevens. Deze leden vinden het daarom zeer schokkend dat medewerkers van de GGD misbruik hebben gemaakt van hun positie en persoonsgegevens wederrechtelijk hebben verkregen, met als doel deze aan te bieden aan derden. Voor deze leden zijn er drie hoofdvragen die zij graag beantwoord zien:
1. Hoe groot is de omvang van het datalek en hoe heeft dit kunnen gebeuren?
2. Wat heeft de Minister gedaan om het lek te stoppen?
3. Hoe informeert de Minister de slachtoffers?

Aanvullend hierop hebben de leden van de VVD-fractie meerdere vervolgvragen.

De leden van de VVD-fractie vragen de Minister welke maatregelen hij had getroffen om datalekken te voorkomen in de systemen van de GGD? Welke aanvullende maatregelen heeft de Minister genomen nadat hij in december aan de Kamer schreef dat er een risico was op datalekken? Klopt het dat de GGD (medische) persoonsgegevens verwerkte, terwijl de organisatie nog niet aan de NEderlandse Norm (NEN)-norm voldeed?

Tijdens het vragenuur op 26 januari jl. stelde de Minister dat van de GGD verwacht mag worden dat sollicitanten aan de voorkant goed worden gescreend, voordat zij worden aangenomen dus. Kan de Minister aangeven hoe deze screening eruitziet en/of dit proces identiek is voor alle medewerkers van de GGD én medewerkers van externe partijen? Klopt het dat medewerkers die niet in het bezit zijn van een verklaring omtrent gedrag (VOG) toegang hebben gehad tot (medische) persoonsgegevens? Klopt het dat medewerkers die in het bezit zijn van een strafblad toegang hebben gehad tot (medische) persoonsgegevens? Hoe kon het gebeuren dat medewerkers zonder VOG (medische) persoonsgegevens konden inzien?

Aan welke voorwaarden moeten medewerkers van de GGD voldoen om toegang te krijgen tot gevoelige informatie? Hoeveel medewerkers voldoen aan deze voorwaarden en wordt gecontroleerd of medewerkers aan deze voorwaarden voldoen? Tot op welk niveau in het systeem hebben medewerkers toegang tot gevoelige data? Kan de Minister voorts

aangeven hoe het autorisatieproces om toegang te krijgen tot gevoelige informatie eruitziet, wie verantwoordelijk is voor het beheer van dit autorisatieproces en wie de eigenaar is van het registratiesysteem? Op welke manier wordt geregistreerd welk persoon welk type gevoelige informatie heeft ingezien? Kan daarbij ook achterhaald worden welke functionaliteiten deze persoon heeft gebruikt tijdens het inzien van deze gevoelige informatie? Zo nee, waarom niet? Waarom hadden niet enkel de medewerkers voor wie dit noodzakelijk was, toegang tot gegevens in persoonsdossiers?

De leden van de VVD-fractie vragen de Minister voorts of het klopt dat de exporteer-functionaliteit inmiddels verwijderd is? Kan de Minister aangeven met welk doel deze functionaliteit ingebouwd is?

Klopt het dat de GGD pas eind maart systemen heeft die automatisch en continu zullen controleren op misbruik? Hoe garandeert de Minister dat de persoonsgegevens van mensen die zich laten testen of vaccineren voortaan veilig zijn?

Gelet op het feit dat ook persoonsgegevens bij het vaccinatieproces geregistreerd en gedeeld worden, en hierbij ook verschillende registratiesystemen aan elkaar gekoppeld moeten worden, willen de leden van de VVD-fractie een klemmende oproep doen om te zorgen dat deze persoonsgegevens zo goed mogelijk beschermd worden. Tijdens het coronadebat over vaccinatie op 17 december jl., stelde de Minister dat er nog veel discussie was over de condities waarbij gegevens kunnen worden gedeeld. Kan de Minister aangeven welke stappen er sindsdien zijn gezet? Zijn er al condities bekend waarbij gegevens gedeeld kunnen worden en zo ja, welke zijn dit?

De leden van de VVD-fractie vragen of er, naast de twee verdachten die nu zijn opgepakt, nog meer mensen verdacht worden van het misbruiken van de informatie van de GGD? Welke acties onderneemt de Minister om de handel in de al buitgemaakte (medische) persoonsgegevens te stoppen? Zijn er signalen van misbruik van de buitgemaakte (medische) persoonsgegevens?

Vragen en opmerkingen van de PVV-fractie

De leden van de PVV-fractie hebben met ontzetting kennisgenomen van de grootschalige handel in persoonsgegevens uit de coronasystemen bij de GGD. Het gaat om privacygevoelige informatie van namen en adresgegevens, telefoonnummers, burgerservicenummers (BSN's) en testuitslagen van miljoenen Nederlandse burgers. Genoemde leden stellen vast dat hier sprake is van een ernstig misdrijf en roepen de Minister op onmiddellijk te zorgen voor een veilig coronasysteem. Daarnaast hebben deze leden de volgende kritische vragen en opmerkingen.

De leden van de PVV-fractie zijn geschokt dat de illegale handel in coronadata al maanden aan de gang is. Hoe kan het zijn dat dit niet eerder is gesignaleerd? Worden er geen steekproeven afgenomen? Waarom zijn nergens alarmbellen afgegaan? Genoemde leden vinden een VOG-verklaring en een geheimhoudingsplicht voor GGD-medewerkers volstrekt onvoldoende als blijkt dat hierop niet actief wordt gehandhaafd. Klopt het dat niet alle medewerkers een VOG-verklaring hebben? Zo ja, om hoeveel medewerkers gaat het? Zo ja, hoe gaat de Minister bewerkstelligen dat zij wel een VOG-verklaring gaan overleggen? Wat gaat de Minister doen om te bewerkstelligen dat medewerkers die geen VOG-verklaring kunnen overleggen niet voorde GGD kunnen werken? Wat de geheimhoudings-

plicht waard is, blijkt wel uit de grootschalige handel die nu aan het licht is gekomen. Welke sanctie staat er op het schenden van de geheimhoudingsplicht en hoe vaak is deze sanctie opgelegd?

De leden van de PVV-fractie vinden dat veel te veel informatie wordt verzameld van burgers. Genoemde leden willen weten welke informatie nu precies in de coronasystemen van de GGD staan en waarom het nodig is om voor een simpele coronatest zoveel informatie op te slaan? Kan de Minister duidelijk maken welke gegevens de GGD vastlegt in het kader van het testen en het bron- en contactonderzoek? Kan de Minister per dataveld aangeven wat de noodzaak is van het registreren van het dataveld in de onderhavige IT-database? Wil de Minister hierbij met name ingaan op de persoonsgebonden velden, zoals het BSN, de NAW-gegevens et cetera? Wat wordt in het kader van een coronatest verstaan onder noodzakelijke informatie? Waarom is de Minister van mening dat de GGD adresgegevens nodig heeft wanneer iemand zelf naar een teststraat toekomt? Waarom is de Minister van mening dat de GGD het BSN-nummer van iemand nodig heeft voor het afnemen van een test? Waarom kan niet worden volstaan met een eenmalige, tijdelijk afgegeven code? Hoe lang worden welke gegevens bewaard? Is bij de bouw van het coronasysteem overleg geweest met deskundigen en privacyexperts over de informatievergaring en de beveiliging daarvan? Zo nee, waarom niet? Wordt de verkregen informatie gedeeld met andere partijen, bijvoorbeeld voor statistische doeleinden? Wat is de bewaartermijn voor de data die wordt vergaard? Bestaat er een koppeling met het medisch dossier of met andere medische gegevens van de betrokken personen? Zo ja, waarom?

Voorts vragen de leden van de PVV-fractie de Minister waarom al deze privacygevoelige informatie toegankelijk is voor minstens 26 duizend GGD-medewerkers. Kan de Minister aangeven hoeveel medewerkers daadwerkelijk toegang hebben tot de genoemde GGD-systemen? Welke noodzaak c.q. bedrijfsbelang is er dat rechtvaardigt dat al deze medewerkers toegang hebben tot de volledige inhoud van de databases? Kunnen al deze medewerkers deze data ook exporteren naar een bestand of andere gegevensdragers? Is er interne controle op wie dit soort specifieke handelingen binnen de database heeft uitgevoerd? Wordt een systeem van persoonsgebonden *logging* van de activiteiten binnen de databases gehanteerd? Hoe vaak wordt hierover intern gerapporteerd naar de directie van de GGD en wanneer gebeurde dit voor het laatst? Wat zijn de interne aanbevelingen geweest en kan de Kamer hier een exemplaar van ontvangen? Klopt het dat het huidige systeem de mogelijkheid biedt te werken met functieprofielen met niveaus van toegankelijkheid, maar dat alle medewerkers gemachtigd zijn en/of waren belangrijke data te exporteren? Zo nee, hoe is de situatie dan wel? Zo ja, hoe kon dit gebeuren? Hoeveel medewerkers zijn en/of waren gemachtigd data te exporteren? Kan de Minister aangeven of en hoe het systeem met veiligheidsniveaus vormgegeven is? Waarom kent het systeem een exportfunctie, waardoor het zo is dat iedere medewerker grootschalig data kan overzetten en versturen? Waarom kan een medewerker uit Groningen bij testuitslagen uit Limburg? Waarom moet het tot eind maart duren voordat het systeem automatisch en permanent gemonitord wordt? Betekent dit dat de illegale handel in coronadata gewoon kan doorgaan?

Zijn er externe IT-deskundigen ingeschakeld die het systeem op dit moment doorlichten op alle mogelijke datalekken? Zo nee, waarom niet? Wanneer is voor het laatst door een externe partij, bijvoorbeeld door een betrokken accountant of een ander gespecialiseerd bedrijf, een IT-systems audit en/of een IT-risk en control framework audit uitgevoerd, om deinterne IT-controlerisico's en bedrijfsrisico's in kaart te brengen? Hoe luidde dit oordeel van de accountant c.q. de auditor? Welke aanbevelingen

zijn gedaan? Wat is het tijdspad van de invoering van deze aanbevelingen en hoe staat het op dit moment met de invoering hiervan? Kan de Kamer een kopie van deze aanbevelingen ontvangen? Als er recent geen IT-audit door een externe partij is uitgevoerd, weet de Minister of de GGD dan voornemens is dit alsnog met spoed te doen? In de berichtgeving wordt gesproken over twee coronasystemen. Hoeveel systemen zijn er in totaal? Wordt via deze systemen allemaal dezelfde informatie verzameld? Per wanneer zijn de systemen veilig? Hoeveel medewerkers zijn inmiddels gecontroleerd en hoeveel onrechtmatigheden zijn inmiddels vastgesteld?

Tot slot vragen de leden van de PVV-fractie aandacht voor de mensen van wie data is gelekt. Kan de Minister een inschatting maken hoeveel mensen daadwerkelijk schade zullen ondervinden van deze illegale handel en of deze personen te maken krijgen met identiteitsfraude, bedreigingen of *stalking*? Zo nee, waarom niet? Kan de Minister achterhalen van hoeveel mensen persoonsgegevens zijn gestolen en/of doorverkocht? Is al over nagedacht hoe deze mensen geholpen kunnen worden? Moeten deze mensen conform de privacywetgeving worden geïnformeerd? Zijn de betrokken personen überhaupt op de hoogte gesteld van de handel in hun data en kunnen zij ergens terecht met vragen hierover? Realiseert de Minister zich dat medische informatie de meest privacygevoelige informatie is die er is? Zo ja, waarom kon dit zo mislopen? Al vele maanden voert de regering campagne die erop gericht is dat mensen zich al met lichte verkoudheidsklachten moeten laten testen. Wat vindt de Minister ervan dat 7 op 8 personen die een coronatest lieten doen enkel verkouden bleken te zijn en niet besmet met het coronavirus, maar nu wel het slachtoffer kunnen worden van identiteitsfraude? Dit doordat de Minister verantwoordelijk is voor een systeem dat een eitje blijkt te zijn voor diefstal van persoonsgegevens.

Vragen en opmerkingen van de CDA-fractie

De leden van de CDA-fractie maken van de gelegenheid gebruik om enkele vragen te stellen over het datalek bij de coronasystemen van de GGD en de illegale handel in privégegevens als gevolg hiervan.

De GGD gaat geautomatiseerd onderzoeken of medewerkers ongeoorloofd in privégegevens van burgers hebben gekeken. De automatische controle moet eind maart klaar zijn. Tot nu toe vonden dergelijke controles steekproefsgewijs plaats.[2] De leden van de CDA-fractie vragen of de Minister kan aangeven waarom niet vanaf dag één automatische controles zijn ingezet. Hadden deze controles, met bijvoorbeeld de casus waarbij een ziekenhuis een forse boete heeft gekregen van de Autoriteit Persoonsgegevens (AP) in het achterhoofd, niet het uitgangspunt moeten zijn?[3]

De leden van de CDA-fractie vragen de Minister welke digitale aanpassingen zijn gedaan aan computers, zodat in het vervolg bijvoorbeeld niet meer gekopieerd kan worden.

De leden van de CDA-fractie vragen wat de Minister intussen heeft gedaan om de governance van het Ministerie van Volksgezondheid, Welzijn en Sport (VWS) met betrekking tot ICT aan te passen, naar aanleiding van de

---

[2] Financieel Dagblad, 26 januari 2021, «Door datalek geplaagde GGD gaat controles op dataverwerking automatiseren» (https://fd.nl/economie-politiek/1371891/door-datalek-geplaagde-ggd-gaat-controles-op-dataverwerking-automatiseren)

[3] Autoriteit Persoonsgegevens, 16 juli 2019, «Haga beboet voor onvoldoende interne beveiliging» (https://autoriteitpersoonsgegevens.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-pati%C3%ABntendossiers)

onvolkomenheden die de Algemene Rekenkamer in haar onderzoek naar het Jaarverslag 2019 constateerde omtrent het incidentmanagement, het bestuur (governance), de organisatie-inrichting en het risicomanagement-.Welke maatregelen zijn daarnaast genomen op het gebied van archivering, naar aanleiding van de eerdere verdwijning van twee harde schijven uit de kluis met daarop gegevens van het donorregister?

In het vragenuur van 26 januari jl. heeft de Minister aangegeven dat «er geen kruid gewassen is» tegen mensen die dit willen doen. De leden van de CDA-fractie vragen of de Minister overleg heeft gehad met bijvoorbeeld telecomproviders die wel in staat zijn strenge maatregelen te nemen ter bescherming van hun netwerk en eveneens niet in de situatie verkeren te kunnen zeggen dat ze niets tegen misbruik kunnen doen? Welke lessen denkt de Minister van hen te kunnen leren?

De Minister heeft aangegeven dat zeker 10 duizend GGD-medewerkers de contactgegevens kunnen inzien van mensen die zich hebben laten testen of vaccineren. De leden van de CDA-fractie vragen de Minister waarom duizenden medewerkers data mogen inzien die voor hen niet relevant is. Dat een team verschillende diensten uitvoert is begrijpelijk, maar medewerkers uit bijvoorbeeld Groningen hebben toch niets van doen met gegevens van mensen uit Goes?

De leden van de CDA-fractie vragen de Minister welke basissystemen gebruikt worden, van welke leverancier deze systemen zijn, en wanneer deze systemen zijn aangekocht.Kan de Minister daarnaast in detail aangegeven welke systemen door de 26 GGD-regio's worden gebruikt, hoe deze aan elkaar zijn gekoppeld, of data bij overdracht zijn versleuteld en zo ja, of dit gebeurt zonder nieuwe versleuteling bij een knooppunt?

Welke civielrechtelijke en/of andere juridische stappen worden genomen tegen deze leverancier? Is deze leverancier alle instructies en voorwaarden van het contract nagekomen met betrekking tot de aanpak van de bescherming van persoonsgegevens of is de leverancier hierin nalatig geweest?

De leden van de CDA-fractie dachten dat testuitslagen slechts enkele weken bewaard zouden worden. Hoe kan het dan zo zijn dat zo veel data op straat zijn komen te liggen?Hoe komt het dat nog niet duidelijk is hoeveel gegevens gestolen zijn?Deze leden vragen verder of er automatische controles zijn omtrent de persoonsgegevens en of in dit kader intussen een extern bureau ingehuurd?

Waarom werd pas in december 2020 een extern bureau ingehuurd om te controleren bij dit proces? Waarom ontbrak de urgentie om de adviezen van dat bureau met spoed te implementeren?

De leden van de CDA-fractie vragen de Minister hoe en wanneer burgers van wie de gegevens gestolen zijn,geïnformeerd worden. Deze leden vragen daarnaast hoe burgers hun gegevens uit de systemen van de GGD kunnen laten verwijderen of anonimiseren.

Het blijkt dat ook data van uitgezonden militairen op straat liggen. De leden van de CDA-fractie vragen de Minister welke maatregelen zijn genomen om deze militairen, die in dienst van ons land in gevaarlijke situaties in het buitenland verkeren, te beschermen.

Volgens RTL heeft de GGD laten weten dat medewerkers een VOG moeten aanleveren en een geheimhoudingsverklaring moeten ondertekenen. De leden van de CDA-fractie vragen de Minister of dit in alle gevallen tijdens

het aannemen van medewerkers is gebeurd, en niet pas nadat medewerkers al enige tijd met de systemen hebben gewerkt.

De leden van de CDA-fractie vragen de Minister of hij kan garanderen dat GGD-medewerkers misstanden intern en desnoods extern kunnen melden zonder dat zij te hoeven vrezen voor represailles.

Vragen en opmerkingen van de D66-fractie

De leden van de D66-fractie zijn verontrust over de illegale handel in grote hoeveelheden gevoelige privégegevens van miljoenen Nederlanders afkomstig uit de slecht beveiligde datasystemen CoronIT en HPzone van de GGD en hebben hierover vragen aan de Minister, in aanloop naar het door de leden van de D66-fractie verzochte Kamerdebat over deze situatie.

De leden van de D66-fractie achten het cruciaal dat zorgvuldig met gevoelige gegevens van burgers wordt omgegaan en dat Nederlanders er van verzekerd zijn dat hun gegevens niet in handen van criminelen terecht kunnen komen. Als gevoelige gegevens niet veilig zijn bij de GGD kan dit grote afbreuk doen aan het vertrouwen in de overheid en het draagvlak voor het coronatestbeleid.

De leden van de D66-fractie hebben achtereenvolgens vragen en opmerkingen over de inhoud en opbouw van de datasets, de bronnen voor de datasets, de toegang tot de datasets, de beveiliging van de systemen, de risico's voor burgers en overige zaken.

De leden van de D66-fractie horen graag van de Minister welke gegevens nu precies per persoon worden vastgelegd en waarom. Waarom zou de GGD bijvoorbeeld het BSN en het adres bewaren van mensen die een coronatest hebben laten doen? Volstaat contactinformatie zoals een telefoonnummer of e-mailadres daarvoor niet? Is het bewaren van grote hoeveelheden gevoelige gegevens wel proportioneel? Is bij de ontwikkeling van de systemen gebruik gemaakt van belangrijke principes als *privacy by design*, dataminimalisatie en doelbinding? Zo nee, waarom niet?

De leden van de D66-fractie vernemen graag hoe de omvangrijke datasets in de systemen nu precies tot stand komen en op basis van welke bronnen ze worden samengesteld. Waar komen de gegevens vandaan? Wie leveren een bijdrage aan de datasets? Met welke private externe organisaties heeft de GGD samengewerkt voor de totstandkoming van de coronasystemen en de datasets?

Ook vernemen de leden van de D66-fractie graag van de Minister hoe de autorisatie en toegang tot de coronasystemen is geregeld. Welke private externe organisaties hebben er naast de GGD-medewerkers allemaal toegang tot de datasets met gevoelige gegevens? Hoeveel mensen kunnen in totaal bij deze gegevens? Op welke wijze verliep de autorisatie? Hoe werden de gegevens tussen de groep(en) mensen met toegang precies gedeeld? Verliep dat volgens Algemene verordening Gegevensbescherming (AVG)-bestendige normen en protocollen? Was ook iedereen bij de betrokken private externe organisaties verplicht om een VOG aan te leveren? Hoeveel mensen hadden toegang tot de coronasystemen zonder een VOG te overleggen? Werd er goed vastgelegd wie op welk moment toegang had tot persoonsgegevens?

De leden van de D66-fractie willen graag precies van de Minister weten hoe de beveiliging van de systemen en datasets georganiseerd is en met welke waarborgen. Welke controles werden uitgevoerd om de databe-

scherming van miljoenen burgers te waarborgen? Is na de berichtgeving van de afgelopen dagen centraal en gestructureerd ingegrepen om dit veilig(er) te laten verlopen?

De leden van de D66-fractie vragen ook aandacht voor het volgende. Het uitlekken van (bijzondere) persoonsgegevens zoals BSN's en woonadressen kan grote risico's als identiteitsfraude, intimidatie en stalken meebrengen voor mensen die in de systemen zijn opgenomen. De leden van de D66-fractie horen graag van de Minister of het mogelijk is om persoonsgegevens uit de systemen van de GGD te laten verwijderen? Zo ja, hoe worden mensen hiervan op de hoogte gebracht? Hoe worden slachtoffers geïnformeerd over de vraag of hun gegevens zijn gestolen en/of doorverkocht? Hoe gaat de GGD volgens de Minister communiceren met bezorgde burgers die overwegen geen coronatest meer te doen?

De leden van de D66-fractie horen graag van Minister welke stappen zijn gezet ten behoeve van de informatiebeveiliging van de coronasystemen na de onthulling in september 2020 van Nieuwsuur dat honderden medewerkers van de coronatestlijn ongewenste toegang hadden tot persoonsgegevens. De Minister meldde toen dat er ook sprake was van steekproeven om te controleren of niet gesjoemeld werd met data. Waarom was er sprake van steekproeven en was er geen bredere controle? Wat waren de uitkomsten van deze steekproeven? Was er vaker sprake van datalekken en/of illegale datahandel met corona-gerelateerde systemen die nog niet bekend zijn gemaakt? Hoe kan het dat grootschalige illegale handel in data afkomstig uit GGD-systemen pas na berichtgeving van RTL op 25 januari jl. naar buiten is gekomen? Klopt het dat er zelfs een grootschalige exportfunctie bestond voor data uit de coronasystemen? Zo ja, waarom is hier überhaupt sprake van geweest?

Afgelopen week kwam nog naar buiten dat het bedrijf U-Diagnostics onzorgvuldig om is gegaan met de persoonsgegevens van defensiemedewerkers. Zo zouden (bijzondere) persoonsgegevens van militairen in WhatsApp-groepen gedeeld zijn. De leden van de D66-fractie vragen de Minister of systemen zoals CoronIT, HPzone en andere systemen bij de GGD of het Ministerie van Volksgezondheid op eenzelfde manier tot stand zijn gekomen en op eenzelfde wijze voor grote aantallen mensen toegankelijk zijn.

De leden van de D66-fractie vragen de Minister tenslotte waarom niet gebruik is gemaakt van de opgedane ervaring rondom de ontwikkeling van de CoronaMelder, waarbij op een zorgvuldige en intensieve wijze, in samenwerking met veel deskundigen en onderzoekers, veel aandacht is besteed aan informatieveiligheid en *privacy by design*. Waarom is van deze expertise geen gebruik gemaakt bij CoronIT en HPzone? Zijn deze coronasystemen in tien maanden tijd verbeterd na de ervaring met de CoronaMelder? Is er geregeld contact geweest met de AP over de risico's met betrekking tot de coronasystemen?

Vragen en opmerkingen van de GroenLinks-fractie

De leden van de GroenLinks-fractie hebben met grote zorg en verbazing kennisgenomen van het grote datalek bij de digitale coronasystemen van de GGD. Het valt niet genoeg te benadrukken dat het voor het vertrouwen van burgers in de overheid essentieel is dat persoonsgegevens veilig verwerkt worden. In de context van de coronabestrijding is het bovendien van het grootste belang dat mensen zich laten testen bij symptomen en actief deelnemen aan bron- en contactonderzoek. Een datalek bij de digitale coronasystemen van de GGD kan ertoe leiden dat burgers terughoudender worden met het aanvragen van testen en deelnemen aan

bron- en contactonderzoek. Dit kan daarmee de coronabestrijding ondermijnen. Wat gaat de ministerin algemene zin doen om het vertrouwen in de systemen van de GGD te herwinnen?

De leden van de GroenLinks-fractie begrijpen uit de beantwoording van mondelinge vragen over dit onderwerp dat de Minister de oorzaak van dit lek vooral zoekt bij de criminele daden van afzonderlijke medewerkers en niet bij de systeembeveiliging. Kan de Minister deze zienswijze verder toelichten? Genoemde leden zijn immers van mening dat er wel degelijk veel te verbeteren valt aan de systemen. De Minister stelt dat medewerkers van de GGD alleen toegang hebben tot persoonsgegevens wanneer dit noodzakelijk is voor het uitvoeren van hun werkzaamheden. Geldt dit ook voor medewerkers van callcenters die in opdracht van de GGD werken? Kan de Minister gedetailleerd uiteenzetten tot welke gegevens een medewerker van een callcenter, die belast is met het inboeken van testafspraken en doorbellen van testresultaten, toegang heeft? Klopt het dat betreffende medewerker toegang heeft tot alle dossiers en niet enkel tot het dossier waar de medewerker op dat moment mee bezig is? Waarom is het noodzakelijk dat een callcentermedewerker toegang heeft tot alle dossiers? Is het systeem dusdanig vorm te geven dat een medewerker enkel toegang heeft tot het dossier waar hij of zij op dat moment mee bezig is, en in geen geval toegang heeft tot dossiers die niet door hem of haar op die dag worden behandeld? Zo ja, waarom zijn de systemen dan niet vanaf het begin op deze wijze vormgegeven? Kan de Minister aangeven welke partijen de digitale coronasystemen hebben ontworpen en welke opdrachten daarbij zijn meegegeven vanuit het Ministerie van VWS en vanuit de GGD? Was volledige inachtneming van het principe van *privacy by design* daar een onderdeel van?

Kunt u voor de systemen CoronIT, HPZone Light en het digitale systeem voor vaccinaties exact aangeven hoeveel mensen toegang hebben tot de gegevens in persoonlijke dossiers? In hoeverre zijn die toegangsrechten al teruggeschroefd? Hoeveel mensen hadden voor die tijd recht op toegang?

Verder vragen de leden van de GroenLinks-fractie de Minister of een callcentermedewerker de mogelijkheid heeft om de gehele database van dossiers te doorzoeken? Zo ja, op welke variabelen kan men dan zoeken? Waarom is dit noodzakelijk voor het uitvoeren van hun werkzaamheden? In de Minister bereid om deze zoekfunctie met onmiddellijke ingang stop te zetten?

De leden van de GroenLinks-fractie zijn ook verbaasd dat callcentermedewerkers toegang hadden tot een exportfunctie waarmee ze gericht konden zoeken naar bepaalde data in de systemen en deze vervolgens grootschalig konden downloaden. Waarom zat deze functie überhaupt in het systeem, zo vragen deze leden aan de Minister? Heeft niemand daar ooit vraagtekens bij geplaatst? Werkten de callcentermedewerkers met toegang tot deze functie vanuit huis of op kantoor op locatie? In het geval van deze laatste situatie: hoeveel mensen werkten op locatie en beschikten de computers van de callcenters over een geactiveerde USB-poort? Kan de Minister garanderen dat medewerkers niet langer de mogelijkheid hebben om data uit de coronasystemen te downloaden en te exporteren?

In dit kader vragen de leden van de GroenLinks-fractie de Minister ook om nadere details van de risicoanalyse op de IT-systemen in de test- en traceerketen. De Minister schreef in de Kamerbrief van 24 december jl. dat naar aanleiding daarvan beter passend autorisatiebeheer zou worden ingericht om het risico op datalekken te minimaliseren. Kan de Minister aangeven hoe dat autorisatiebeheer er voorheen uitzag, welke verande-

ringen er zouden worden doorgevoerd naar aanleiding van de risico-analyse en in hoeverre dat al is gebeurd? Vormt de recente berichtgeving van RTL over enorme datalekken aanleiding om dat autorisatiebeheer verder aan te scherpen? Zo nee, waarom niet? Zo ja, op welke wijze?

Ook vragen deze leden of en zo ja, op welke wijze deze risicoanalyse is gedeeld met de AP. In hoeverre heeft de AP daar kritisch naar kunnen kijken en commentaar op kunnen leveren? Wat is er gebeurd met het commentaar? Kan de Minister ook aangeven in hoeverre de digitale coronasystemen in een eerder stadium zijn onderworpen aan een Privacy Impact Assessment of een andere privacy risico-inventarisatie? Wat waren de uitkomsten hiervan, zijn deze gedeeld met de AP en heeft de AP hier kritisch naar kunnen kijken en commentaar op kunnen leveren? Zo ja, wat is daarmee gedaan? Zo nee, waarom niet? Voorts vragen de leden van de GroenLinks-fractie de Minister of alle data die momenteel wordt verzameld daadwerkelijk noodzakelijk is. Kan de Minister uitleggen waarom de GGD zowel adresgegevens als BSN's nodig heeft? Wat is het huidige beleid van de GGD met betrekking tot de verwijdering en pseudonimisering van persoonsgegevens? Welke afwegingen worden hierbij gemaakt? In hoeverre hebben burgers de mogelijkheid om hun gegevens in de systemen van de GGD te laten verwijderen of te laten pseudonimiseren?

De leden van de GroenLinks fractie hoorden de Minister benadrukken dat het kabinet inzet op extra maatregelen om de pakkans te vergroten en dat er meer controles zullen worden uitgevoerd die tevens worden geautomatiseerd. De Minister schreef echter in antwoord op schriftelijke vragen naar aanleiding van een uitzending van Nieuwsuur in september al dat er scherpe controle plaatsvindt op de *logging*, door nauwlettend bij te houden welke dossiers door wie worden ingezien. Hoe kan het dan dat er toch grootschalig data zijn ingezien en uitgelekt? Hoe werken die controles precies? Op welk moment gaat er een alarmbel af? Zien de controles enkel toe op toegang tot dossiers, of ook op zoekopdrachten? Kan de Minister aangeven of het klopt dat de GGD alleen steekproefsgewijs controles uitvoert? Zo ja, kan de Minister aangeven waarom dit zo is? Kan de Minister aangeven of het klopt dat momenteel geen enkele waarschuwing wordt afgegeven, noch aan de medewerker zelf, noch aan de systeembeheerder, wanneer een medewerker een dossier opent waar hij of zij niet aan werkt of een onnodige zoekopdracht uitvoert? Wat waren de bevindingen van de risicoanalyse met betrekking tot de controlesystemen en stonden er ook op dat vlak extra maatregelen gepland? Hoe staat het daarmee?

Met betrekking tot de screening van medewerkers geeft de Minister aan dat alle mensen die de GGD aanneemt in bezit moeten zijn van een geldige VOG. Geldt dit ook voor callcentermedewerkers die niet in dienst zijn, maar wel in opdracht van de GGD werken en daarbij toegang hebben tot gevoelige persoonsgegevens? Zo ja, hoe ziet de GGD erop toe dat zijn een VOG overleggen? Zo nee, waarom niet?

Ook vragen de leden van de GroenLinks-fractie de Minister in hoeverre de opsporingsdiensten zich bezighouden met het bestrijden van illegale datahandel? Hoe is het mogelijk dat de autoriteiten deze grootschalige handel in gegevens uit veelomvattende nieuwe (en dus risicovolle) GGD-systemen nog niet op het spoor waren en daarop moesten worden gewezen door een journalist? Is er zicht op verdere arrestaties van mensen die dit datalek hebben geëxploiteerd? Is daarbij alleen aandacht voor handelaren die de data hebben aangeboden, of gaat men ook op zoek naar individuen die deze illegale datasets hebben gekocht?

De leden van de GroenLinks-fractie zijn uitermate bezorgd over de mogelijke gevolgen van het vastgestelde datalek voor de slachtoffers, zoals identiteitsfraude en oplichting. Kan de Minister op deze zorgen ingaan? Welke mogelijke gevolgen ziet de Minister en wat wordt ondernomen om de risico's hiervan te mitigeren? Deze leden horen zorgwekkende berichten van verschillende GGD'en dat kwetsbare ouderen worden gebeld door mensen die zich voordoen als GGD-medewerkers en vervolgens worden opgelicht. Hoeveel van deze gevallen zijn bekend bij de regering? In hoeverre kunnen deze gevallen van oplichting een verband houden met het datalek bij de GGD? Heeft het datalek de kans op dit soort misstanden vergroot?

In het kader van het mitigeren van de risico's zijn de leden van de GroenLinks-fractie voorts van mening dat het essentieel is om iedereen die mogelijk slachtoffer is geworden van dit datalek daarover zo spoedig mogelijk te informeren, zodat men alert kan zijn op verdachte signalen die kunnen wijzen op misbruik van gestolen persoonsgegevens. Deelt de Minister deze mening en komt hij daarmee ook tot de conclusie dat men daar niet mee kan wachten tot de uitkomsten van strafrechtelijke en forensische onderzoeken bekend zijn? Zo nee, waarom niet? Zo ja, op welke wijze en op welke termijn gaat de Minister de mogelijke slachtoffers informeren? Klopt het dat iedere Nederlander die zich heeft laten testen of is benaderd bij bron- en contactonderzoek mogelijk slachtoffer is? Heeft de regering al een idee van het geschatte aantal daadwerkelijke slachtoffers? Is de Minister bereid om, in lijn met het advies van de AP, een speciale GGD-informatielijn op te zetten voor bezorgde burgers?

Deelt de Minister voorts de mening dat wachten met informeren van de mogelijke slachtoffers ook niet in overeenstemming zou zijn met de «Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679» van de Europese Commissie?[4]. Zo nee, kan de Minister dat toelichten onder verwijzing naar Hoofstuk III van de richtsnoeren?

Vragen en opmerkingen van de SP-fractie

De leden van de SP-fractie hebben verschillende opmerkingen en vragen over het datalek bij de coronasystemen van de GGD en de vermoedelijke handel in privégegevens van miljoenen Nederlanders uit deze systemen. Zoals op 26 januari jl. tijdens het vragenuur ook is aangegeven, vinden genoemde leden dit een ernstige situatie. Deze leden zijn dan ook van mening dat snelle en complete duidelijkheid essentieel is en dat het vertrouwen onder de Nederlandse bevolking in deze systemen hersteld moet worden.

Allereerst vragen de leden van de SP-fractie welke acties zijn genomen nadat Nieuwsuur in september vorig jaar bekend maakte dat honderden testlijnmedewerkers bij alle persoonsgegevens konden, terwijl daar geen noodzaak toe was? Kan chronologisch worden uiteengezet op welk moment welke maatregelen sindsdien zijn genomen om persoonsgegevens beter te beschermen?

Kan de Minister aangeven waarom in het ontwerp van de gebruikte software niet meer maatregelen zijn ingebouwd om persoonsgegevens beter af te schermen? Is de mogelijkheid van het (gedeeltelijk) pseudoni-

[4] Autoriteit Persoonsgegevens, 6 februari 2018, «Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679» (https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_meldplicht_datalekken.pdf)

miseren van gegevens bij de ontwikkeling van de software overwogen? Waarom is hier niet voor gekozen, denk bijvoorbeeld aan het afschermen van BSN's? Op welke wijze worden rechten voor het inzien van bepaalde data afgegeven en hoe wordt hierbij voorkomen dat gebruikers meer informatie te zien krijgen dan strikt noodzakelijk is? Hoe kan het dat 26 duizend mensen toegang hebben tot een bestand waarin privacygevoelige informatie van honderdduizenden Nederlanders te vinden is? Zijn hier tijdens het ontwerp en tijdens de ontwikkeling van de software niet al grove fouten gemaakt?

Klopt de informatie die de leden van de SP-fractie ter ore is gekomen dat gebruikers van CoronIT of HPZone vergaande aanpassingen kunnen of konden doen in bijvoorbeeld het onderdeel dat de resultaten van het laboratoriumonderzoek weergeeft? Klopt het dat medewerkers die verder niks met het laboratoriumonderzoek te maken hebben gehad op afstand wijzigingen kunnen aanbrengen in het gebruikte afnamemateriaal (swab of speekselspons).

Wat vindt de Minister ervan dat door de GGD en samenwerkende partijen privacygevoelige informatie is uitgewisseld in WhatsApp-groepen? Is dit een veilige manier om informatie te delen en hoe verhoudt zich dit met geldende wet- en regelgeving? Klopt het dat het oorspronkelijk bedoeld was te communiceren via het programma RocketChat, maar dat dit systeem dusdanig vaak vastloopt dat breed gebruik is gemaakt van WhatsApp? Wat vindt de Minister hiervan? Wordt op dit moment wel naar behoren gecommuniceerd?

Kan een lijst worden overlegd van de publieke en private organisaties die toegang hebben tot CoronIT en HPZone en aan worden gegeven welke organisaties gemachtigd waren om accounts aan te maken om data te lezen of toe te voegen aan beide systemen? Wie of welke organisatie draagt de eindverantwoordelijkheid voor het geven van rechten aan organisaties voor het werken met beide programma's?

In de beantwoording op onze eerdergenoemde mondelinge vragen is aangegeven dat RTL de GGD heeft getipt over de illegale datahandel. De leden van de SP-fractie zijn van mening dat dit geen correcte weergave van de werkelijkheid is. Is de Minister het eens met genoemde leden dat RTL kritische vragen heeft gesteld in plaats van dat de GGD door hen is getipt? Zo ja, kan de Minister inzicht geven in de gestelde vragen en antwoorden? Kan de Minister in een overzicht aangeven welke wijzigingen aan zowel CoronIT als HPZone zijn aangebracht als gevolg van de vragen die door RTL zijn gesteld? Klopt het bijvoorbeeld dat de exportfunctie, die het grootschalig delen van data een stuk eenvoudiger maakt, pas uitgeschakeld is nadat hier door RTL vragen over zijn gesteld?

De leden van de SP-fractie vragen de Minister om een compleet overzicht in de omvang van het datalek. Indien dit overzicht er niet is, vragen deze leden om een tussenstand en vragen deze leden tevens per wanneer dit overzicht wel volledig beschikbaar is? Daarnaast vragen genoemde leden of dit overzicht direct naar de Kamer gestuurd kan worden wanneer deze gereed is?

De leden van de SP-fractie krijgen graag een precies overzicht van de ontstane situatie. Is het bijvoorbeeld duidelijk in welke systemen sprake is van datadiefstal? Is het correct dat dit naast CoronIT ook geldt voor het systeem HPZone, een systeem waar ook medische gegevens worden geregistreerd? Zo ja, welke extra risico's brengt dit volgens de Minister met zich mee en welke specifieke maatregelen worden naar aanleiding hiervan genomen?

Hoeveel mensen hebben exact toegang tot de persoonsgegevens die zijn opgeslagen in CoronIT? Klopt het dat dit ongeveer 26 duizend mensen zijn en niet een paar duizend zoals door de Minister werd gesteld tijdens het vragenuur van 26 januari jl.?

Hoeveel mensen hebben exact toegang tot de persoonsgegevens die zijn opgeslagen in HPZone? De leden van de SP-fractie vragen de Minister of gegarandeerd kan worden dat alle medewerkers die toegang hebben tot deze systemen (nu en in het verleden) een VOG en dus geen strafblad hebben? Kan de Minister via een overzicht aangeven hoeveel mensen een VOG hebben overlegd aan de GGD en hoeveel niet? Kan dit ook worden gedaan voor de partners waarmee de GGD samenwerkt of heeft samengewerkt?

De leden van de SP-fractie zijn van mening dat het betreffende systeem volledig veilig dient te zijn, en hebben hierover ook enkele vragen.

In zijn beantwoording van de mondelinge vragen van 26 januari jl. is door de Minister aangegeven dat de GGD sinds de start van de coronapandemie continu de systemen controleert. De leden van de SP-fractie horen graag van de Minister of het klopt dat dit niet het geval blijkt te zijn en dat slechts af en toe een steekproef wordt gedaan. Klopt het volgens de Minister dat de GGD pas na de melding RTL heeft nagedacht over continue geautomatiseerde controles?

Worden zoekopdrachten naar specifieke personen gelogd en gecontroleerd? Is er een waarschuwingsmechanisme van kracht voor het geval de gegevens van bepaalde personen worden opgezocht zonder dat hier noodzaak toe is?

Klopt het volgens de Minister dat CoronIT pas sinds kort aan de NEN-7510-norm voldoet? Hoe is het volgens de Minister mogelijk dat het systeem voldoet aan deze NEN-norm, maar het datalek desondanks niet eerder is opgemerkt? Deelt de Minister de mening dat meer controles het systeem niet direct veiliger maken, maar dat enkel de pakkans van kwaadwillenden hiermee vergroot wordt? Op welke wijze worden de computersystemen daadwerkelijk veiliger gemaakt? Hoe wordt het vertrouwen in deze systemen hersteld?

De leden van de SP-fractie vinden het ernstig dat mensen misbruik van persoonlijke gegevens (kunnen) maken. Welke maatregelen worden volgens de Minister genomen om de handelaars in persoonsgegevens én de eventuele kopers van deze persoonsgegevens op te sporen? Welke acties worden ondernomen om te achterhalen wie in de afgelopen maanden nog meer data uit de GGD-systemen hebben onttrokken?

Kan de Minister ook reageren op de uitspraken van de AP en de vele meldingen die zij hebben binnengekregen van burgers die vrezen dat hun gegevens verhandeld zijn?

De leden van de SP-fractie vragen de Minister of het datalek ook gevolgen heeft voor de registratie van vaccinaties? Hoe wordt hier precies mee omgegaan? Hoeveel mensen hebben toegang tot deze gegevens? Klopt het dat de Minister eerder heeft gesteld dat medewerkers die testafspraken inplannen niet de mogelijkheid hebben om naar de afspraken voor vaccinaties te kijken, maar dat deze medewerkers wel de ingeplande afspraken voor vaccinaties kunnen zien en zij derhalve kunnen zien of iemand wel of niet gevaccineerd is?

Vragen en opmerkingen van de Partij voor de Dieren-fractie

De leden van de Partij voor de Dieren-fractie maken zich grote zorgen over de volstrekt gebrekkige omgang met (medische) privégegevens bij de GGD. Daarnaast zijn deze leden verontwaardigd over de onvolledige en incorrecte wijze waarop de Minister de Kamer hier bij het vragenuur van 26 januari jl. over informeerde.

De leden van de Partij voor de Dieren-fractie hebben de afgelopen jaren al regelmatig gewezen op de gebrekkige infrastructuur die gebruikt wordt bij de digitalisering van de zorg. Zij zijn daarom ook niet verrast dat het hier is misgegaan. Het belang van privacy en het veilig houden van de (medische) gegevens sneuvelt telkens wanneer andere belangen zich aandienen. De fundamentele fout die gemaakt wordt, is dat het beschermen van privacy gezien wordt als iets wat afgewogen kan worden tegenover andere belangen. De bescherming van medische gegevens en het waarborgen van de privacy zou echter een harde randvoorwaarde moeten zijn. Kan een bepaald systeem daar niet aan voldoen? Dan kan het volgens deze leden in principe niet ingevoerd worden.
Kan de Minister bevestigen dat een systeem dat niet ontworpen is vanuit de gedachte om de privacy maximaal te beschermen een slecht systeem is en daarom aangepast of vervangen zou moeten worden?

De leden van de Partij voor de Dieren-fractie hebben verschillende vragen en opmerkingen over het concrete voorval bij de GDD. Genoemde leden vinden het zeer verontrustend dat dit zo mis heeft kunnen gaan. Mensen moeten zich kunnen laten testen zonder dat zij zich daarbij zorgen moeten maken of dieven er met hun gegevens vandoor kunnen gaan, met alle zeer kwalijke gevolgen van dien. Hoe gaan we ervoor zorgen dat het niet zo is dat minder mensen zich laten testen de aankomende tijd? Hoe gaan we zo snel mogelijk alle mensen waarvan de gegevens zijn gestolen op de hoogte brengen?
Kan de Minister bevestigen dat de GGD nog geen enkel idee heeft van de omvang van het lek en het mogelijke misbruik? Klopt het dat de GGD nog niet eens weet welke systemen kwetsbaar zijn en welke niet? Zo ja, wat is de reactie van de Minister daarop en wat gaat de Minister aan doen?

De leden van de Partij voor de Dieren-fractie vragen of de Minister kan aangeven of de werkwijze, zoals beschreven in het RTL-artikel, inmiddels onmogelijk is gemaakt? Op welke wijze is ingegrepen in de fysieke infrastructuur van de ICT-systemen? Welke aanpassingen zijn gedaan aan welke specifieke systemen? Welke andere kwetsbaarheden zijn ontdekt? Welke signalen waren er al voor de publicatie van RTL bij de GGD dat de veiligheid van de medische gegevens absoluut niet gewaarborgd kon worden? Wat is er met die signalen gebeurd?

De leden van de Partij voor de Dieren-fractie vragen de Minister hoe het kan gebeuren dat terwijl de systemen niet op orde zijn de GGD-GHOR op haar website zet; «We zorgen ervoor dat we werken met veilige systemen. We testen dat of we laten dat doen.»[5] Op welke manier is getest of de systemen veilig waren? Wat was dan de uitkomst van die testen? Genoemde leden ontvangen graag deze testresultaten.

In het vragenuur gaf de Minister aan dat de beveiliging van de systemen onvoldoende was en nu is aangescherpt. Allereerst zijn de leden van de Partij voor de Dieren-fractie van mening dat de beveiliging slechts de laatste schil om het systeem zou moeten zijn en dat het systeem qua

[5] GGD GHOR, «Wie werken er met jouw persoonsgegevens?» (https://ggdghor.nl/privacyverklaring-coronit/)

opzet al veel veiliger zou moeten zijn. Genoemde leden hebben ook enkele vragen over de beveiliging. De Minister zei dat deze beveiliging voldoet aan de laatste NEN-norm. Bedoelt de Minister dan alleen de NEN 7510? Of bedoelt de Minister ook de subnorm NEN 7512 aangezien de GGD, het Rijksinstituut voor Volksgezondheid en Milieu (RIVM) en callcenters ook gegevens met elkaar uitwisselen?
Over de NEN 7512 merkte de Partij voor de Dieren in 2019 al op dat die onvoldoende veilig is.[6] Een constatering die later door een kamerbrede meerderheid gesteund werd via een motie die verzocht om te kijken of bijvoorbeeld minimaal end-to-end encryptie ingevoerd kon worden.[7] De Minister gaf in reactie op die motie aan dat in het eerste kwartaal van 2021 de NEN-norm herzien zou zijn. Is dat inmiddels het geval? Wanneer is de NEN 7510 voor het laatst herzien? Als ook de NEN 7512 hier betrekking heeft en de systemen aan de «laatste NEN-norm» voldoen, om welke norm gaat dat dan? De oude norm waarvan al geconcludeerd was dat die onvoldoende veilig was of de nieuwe die in dit kwartaal klaar zou zijn?

Klopt de berichtgeving dat een groot aantal medewerkers bij de GGD en de callcenters geen VOG heeft overlegd? Kan de Minister aangeven waarom hij dan bij het vragenuur meermaals aangaf dat medewerkers een VOG moeten overleggen? Was hij er niet van op de hoogte dat dit niet gebeurd? Kan de Minister aangeven hoe het kan gebeuren dat er mensen waren die geen VOG konden overleggen en wel een strafblad blijken te hebben, toch toegang kregen tot de medische privégegevens van vele duizenden mensen?

Kan de Minister aangeven wat hij bedoelt met de uitspraak «Sinds de start van de pandemie controleert de GGD uiteraard continu het gebruik van de systemen»? Wat wordt bedoeld met het woord «continu»? Is er een vorm van continu toezicht? Zoals het tracken van de handelingen die medewerkers doen? Of is er af en toe een steekproef en vindt deze steekproef met enige continuïteit plaats?
Deelt de Minister de mening van de leden van de Partij voor de Dierenfractie dat steekproeven geen vorm van «continu toezicht» zijn? Zo nee, waarom niet?
De Minister gaf verder in zijn verweer aan: «De mensen die werken bij de GGD hebben alleen toegang tot persoonsgegevens wanneer dit noodzakelijk is.» Kan de Minister bevestigen dat medewerkers ook wanneer dit niet noodzakelijk was gewoon fysieke toegang tot de systemen hadden? Kan de Minister, indien dit het geval is, aangeven waarom hij de Kamer vertelde dat dit niet zo was?
De leden van de Partij voor de Dieren-fractie vragen de Minister in zijn antwoord op bovenstaande vraag niet te verwijzen naar het gegeven dat medewerkers wettelijk gezien geen toegang hadden. Het gaat hier niet om de wettelijke toegang maar de fysieke toegang. Oftewel, de fysieke mogelijkheid om de gegevens in te zien en te downloaden.

Dit punt, het kunnen downloaden van gegevens, is een andere zorg van de leden van de Partij voor de Dieren-fractie. Kan de Minister aangeven welke ICT-systemen die gebruikt worden bij de bestrijding van het coronavirus een zogeheten exportfunctie hebben (gehad)? Kan de Minister aangeven hoeveel medewerkers (niet het aantal fte, maar aantal medewerkers) toegang hadden tot elk van de gebruikte systemen? Kan de

---

[6] Partij voor de Dieren, 30 januari 2019, «Bijdrage Teunissen AO Gegevens uitwisseling in de zorg / gegevensbescherming» (https://www.partijvoordedieren.nl/bijdragen/bijdrage-teunissen-ao-gegevensuitwisseling-in-de-zorg-gegevensbescherming)

[7] Partij voor de Dieren, 20 februari 2019, «Motie Van Kooten-Arissen over versleuteling van berichten in zorgcommunicatie» (https://www.partijvoordedieren.nl/moties/motie-van-kooten-arissen-over-versleuteling-van-berichten-in-zorgcommunicatie)

Minister aangeven hoeveel gegevens/dossiers voor het merendeel van die medewerkers in te zien waren? Kan de Minister via het geven van een getal ook aangeven hoeveel medewerkers toegang hadden tot een exportfunctie? Was er enige vorm van toezicht op het gebruik van die exportfunctie (*logging*)? Kan de Minister aangeven waarom deze exportfunctie was ingevoegd? Welk doel diende deze functie en waarom was de toegang ertoe niet verder beperkt?

Kan de Minister reflecteren op zijn uitspraak: «De GGD heeft uiteraard alles gedaan wat nodig en mogelijk is om de systemen verder te beveiligen»? Staat hij nog altijd achter de bewering dat alles gedaan is wat nodig was?

Voor de leden van de Partij voor de Dieren-fractie is de inzet van de Minister op dit moment niet voldoende. De Minister geeft aan dat medewerkers alleen toegang tot de systemen hebben wanneer dat noodzakelijk is. Dat is incorrect en niet voldoende gewaarborgd. De Minister kan niet enkel blijven vertrouwen op het goede gedrag van de callcenter- en GGD-medewerkers. Het systeem moet ingericht zijn om ook bij overtredingen of misstanden de privacy van mensen zo goed als mogelijk te waarborgen.
Is de Minister bereid te kijken in hoeverre het bestaande systeem en de werkwijze daarvoor kan worden aangepast? Is de Minister bereid te kijken of het systeem en de werkwijze zo kunnen werken dat a) zo min mogelijk medewerkers toegang nodig hebben, b) medewerkers die toegang hebben, toegang hebben tot zo min mogelijk gegevens, c) de toegang expliciet niet mogelijk is wanneer deze ook niet nodig is, d) er een continue controle is op welke gegevens door wie geraadpleegd worden en e) de beveiliging van de systemen op het hoogst denkbare niveau is? Is de Minister bereid deze stappen te nemen? Zo ja, op welke termijn gaat dit lukken?

Is de Minister bereid om voor de stappen die genomen moeten worden de kennis en kunde die in het afgelopen jaar werd aangetrokken weer in te zetten? De leden van de Partij voor de Dieren-fractie zagen bijvoorbeeld dat dat na aandringen bij de ontwikkeling van de CoronaMelder een sterke focus op privacy ontstond. Wat deze leden betreft hoort deze focus standaard te zijn.

De leden van de Partij voor de Dieren-fractie vragen de Minister verder naar de verantwoordelijkheid voor de verwerking van deze gegevens. De Minister verwees hierbij in de Kamer naar de individuele instellingen. Elke instelling is verantwoordelijk voor haar eigen systemen. Kan de Minister aangeven wie er verantwoordelijk was voor de systemen die hier gebrekkig zijn gebleken? Kan de Minister aangeven op welk moment het zijn verantwoordelijkheid wordt? Hoeveel voorvallen in de zorg moeten er nog zijn voordat eindelijk eens grondig de bezem door alle systemen heen gaat? De voorbeelden zijn legio en de zorg is al jarenlang de sector met de meeste datalekken, blijkt uit de jaarrapportages van de AP. Op welk moment gaat de Minister beseffen dat er iets fundamenteel mis is en de huidige visie en werkwijze tekortschiet?

Een van de voorbeelden waar het ook niet goed gaat en waar dezelfde problematiek speelt als bij de GGD-systemen is de Corona opt-in. Normaal gesproken moet voor het inzien van medische gegevens expliciete toestemming zijn gegeven. Tijdens de eerste golf van de coronacrisis heeft de Minister dit aangepast. Vanaf dat moment konden de dossiers ook worden ingezien van mensen die niet hebben aangegeven of ze toestemming geven voor de inzage van hun medische dossiers. Daarmee werden 8 miljoen medische dossiers fysiek toegankelijk voor

heel veel mensen die daar niets mee te maken hebben. Kan de Minister aangeven waarom deze maatregel, die werd ingesteld toen er noodtenten voor de spoedeisende hulp stonden, nu nog altijd nodig is? Had in de tussentijd geen andere oplossing gevonden kunnen worden? Is de AP nog altijd akkoord met deze uitzondering? Is de Minister bereid de AP opnieuw om een advies te vragen op dit punt? Zo nee, waarom niet?

Kan de Minister bevestigen dat, net zoals bij de GGD, bij de Corona opt-in een ongelofelijke hoeveelheid mensen fysiek toegang hebben tot de medische gegevens (meer dan 8 miljoen dossiers) waar zij niets mee van doen hebben? Kan de Minister bevestigen dat ook hier nauwelijks toezicht is of de inzage in deze gegevens rechtmatig en met toestemming plaatsvindt? Kan de Minister de Kamer laten weten op welke manier nu toezicht gehouden wordt op de raadplegingen en of deze rechtmatig zijn? Is het denkbaar dat ook hier gegevens op verzoek verkocht worden? Welke zekerheid heeft de Minister dat dit niet het geval is?
Ziet de Minister de parallel tussen de problematiek bij de GGD, de Corona opt-in en bijvoorbeeld het verhaal waarover NRC schreef op 6 december jl.[8]? Dit zijn allemaal voorbeelden van ICT-systemen in de zorg waarbij de toegang tot medische gegevens veel te ruim is geregeld en het toezicht op de inzage gebrekkig is of ontbreekt. Ziet de Minister in dat het Landelijk Schakelpunt precies dezelfde tekortkoming kent en daarom de welhaast onoplosbare problematiek van de Gespecificeerde Toestemming voortbrengt? Is de Minister bereid de huidige plannen voor de (verdere) digitalisering van de zorg op dit moment in ieder geval niet verder door te zetten? Is de Minister bereid om de omgang met medische gegevens radicaal te gaan herzien vanuit het belang van privacy? Alles minder dan dit is naar de mening van de leden van de Partij voor de Dieren-fractie slechts dweilen terwijl de kraan nog loopt.

Vragen en opmerkingen van de SGP-fractie

De leden van de SGP-fractie maken zich ernstig zorgen over het grote datalek bij de GGD en het feit dat uit journalistiek onderzoek van RTL is gebleken dat er wordt gehandeld in privégegevens van miljoenen Nederlanders. Het lek in CoronIT en HPzone is zeer schadelijk voor de testbereidheid en daarmee in potentie een grote bedreiging voor de coronabestrijding van het kabinet.

Omvang

De leden van de SGP-fractie vragen aan de Minister van hoeveel Nederlanders inmiddels persoonsgegevens in CoronIT of HPzone zijn geregistreerd. Kan de Minister de aard en omvang van het datalek gedetailleerd toelichten en daarbij ingaan op welk soort (persoons)gegevens het betreft en om hoeveel mensen het gaat? Is er duidelijkheid over welke partijen deze gegevens inmiddels in hun bezit hebben? Zo nee, wanneer wordt hier meer over bekend?

Kan zo gedetailleerd mogelijk worden aangeven welke GGD-medewerkers toegang hebben of hadden tot welke informatie en om hoeveel medewerkers het gaat? Zijn er naast de GGD-medewerkers nog andere betrokken partijen die toegang hebben (gehad) tot deze systemen? Hoe is de toegang tot de systemen beveiligd? Welke waarborgen zijn en worden hiervoor gebruikt?

---

[8] NRC Handelsblad, 6 december 2020, «Haar medische gegevens las ze terug in een roman» (https://www.nrc.nl/nieuws/2020/12/06/haar-medische-gegevens-las-ze-terug-in-een-roman-a4022814)

Beveiliging

Kan de Minister in een tijdlijn aangeven welke stappen vanaf maart 2020 zijn gezet om de IT-systemen van de GGD te beveiligen en te testen op risico's? De Minister stelt dat de GGD-systemen volautomatisch acteren. Welke *controls* waren er om dit soort grootschalige data diefstal te voorkomen? Wordt er bijvoorbeeld «gelogd» welke medeweker welke data opvraagt (op deze manier zijn daders te identificeren)? Welke mogelijkheden en *controls* zijn er via systeembeheer om inzichtelijk te maken op welke concrete schaal *data exports* zijn verzonden via sociale media, Wetransfer en/of Onedrive. Diverse eerdere keren is melding gemaakt over de werking van de GGD-systemen en van problemen en issues. Hier schijnt beperkt iets mee gedaan te zijn. Welke meldingen zijn gedaan? Waarom is hier in beperkte opvolging aan gegeven? Wie is verantwoordelijk voor de slechte opvolging van deze meldingen?

Gevolgen

De belangrijkste zorg van de leden van de SGP-fractie betreft het uitlekken van gevoelige persoonsgegevens, met name BSN's en woonadressen. Klopt het dat zeer veel mensen toegang hadden tot de meest persoonlijke en vertrouwelijke gegevens, waaronder het BSN, geboortedata, adresgegevens?

De leden van de SGP-fractie maken zich zorgen over identiteitsfraude, zeker omdat ook veel oudere Nederlanders zijn getest. Is het zo dat de informatie in de IT-systemen na enige tijd automatisch vervalt of wordt verwijderd? Is het mogelijk om deze gevoelige informatie uit de systemen te verwijderen?

Wanneer wordt duidelijk of er al sprake is geweest van identiteitsfraude, diefstal of *stalking*?

Welke overige maatregelen zijn nodig? Wordt momenteel overlegd met banken en andere instanties over het aanpassen van hun protocollen voor identiteitsverificatie?

Is er een publiekscampagne nodig met voorlichting over kwetsbaarheden, zodat mensen (waaronder ouderen) minder snel misleid worden?

Welke mogelijkheden biedt de GGD (en andere instanties die zich met de volksgezondheid bezighouden) aan burgers om te zien welke data de betreffende instantie van hen heeft? In welke mate is het mogelijk om gegevens te verwijderen en/of te anonimiseren?

Is het nodig dat er voor alle Nederlanders een nieuw BSN-nummer wordt aangemaakt, omdat het om miljoenen burgers gaat die de afgelopen maanden zijn getest en totaal onduidelijk is hoeveel persoonsgegevens er inmiddels zijn verhandeld?

Welke risico's heeft dit datalek voor de (staats)veiligheid, bijvoorbeeld wanneer blijkt dat persoonsgegevens van politici, militairen, medewerkers van inlichtingendiensten en/of politieagenten openbaar zijn?

Transparantie

Kan de Minister aangeven of het klopt dat de GGD medewerkers onder druk heeft gezet om geen openheid van zaken te geven, of om niet meer met journalisten te praten? Erkent de Minister dat het in deze situatie cruciaal is om zoveel mogelijk transparantie te geven over wat er is

gebeurd en welke risico's er op dit moment zijn? Kan de Minister een anoniem loket opzetten waar GGD-medewerkers hun inzichten kunnen delen?

II. Reactie van de Minister