AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

GGD GHOR Nederland
t.a.v. de heer A. Rouvoet
Zwarte Woud 2
3524 SJ Utrecht

Datum
8 november 2021

Ons kenmerk
z2021-02000

Contactpersoon
[....]
070 8888 500

Onderwerp
Eindbrief onderzoek beveiliging persoonsgegevens GGD GHOR en GGD'en

Geachte heer Rouvoet,

Naar aanleiding van het op 22 januari 2021 door GGD GHOR Nederland (hierna: GGD GHOR), mede namens de regionale GGD'en aan de Autoriteit Persoonsgegevens (hierna: AP) gemelde datalek, de zorgwekkende berichtgeving in de media over de diefstal van en handel in persoonsgegevens afkomstig uit de systemen van GGD GHOR en de GGD'en alsmede de vele bezorgde signalen die de AP hierover vervolgens ontving, heeft de AP aangekondigd het toezicht op de GGD te intensiveren en in dat kader onderzoek te doen. De AP heeft onderzocht of door GGD GHOR en twee onderzochte GGD'en passende technische en organisatorische maatregelen zijn getroffen om de persoonsgegevens die worden verwerkt in het kader van het testen, vaccineren en bron- en contractonderzoek in verband met de coronapandemie passend te beveiligen. Met deze eindbrief informeert de AP u over de bevindingen van het onderzoek.

De AP is zich ervan bewust dat met het uitbreken van de pandemie de GGD'en en GGD GHOR voor een enorme opgave werden gesteld. Zij kregen de opdracht in zeer korte tijd zorg te dragen voor het op grote schaal testen van personen, het uitvoeren van bron- en contactonderzoek en het vaccineren van personen. De werkzaamheden om dit te realiseren werden onder grote tijdsdruk verricht.

Tegelijkertijd geldt dat van een uitzonderlijk grote groep burgers in dit verband bijzondere persoonsgegevens betreffende hun gezondheid werden en worden verwerkt en dat een grote groep, veelal speciaal voor dit doel aangetrokken, tijdelijke medewerkers hiertoe toegang hebben. Het treffen van technische en organisatorische maatregelen die zijn afgestemd op de hiermee gepaard gaande risico's voor de persoonsgegevens is dan ook van zeer groot belang. De bereidheid van burgers om zich te laten testen en vaccineren of medewerking te verlenen aan bron- en contactonderzoek hangt immers ook samen met

het vertrouwen in de wijze waarop in dat kader persoonsgegevens van burgers worden verwerkt en beveiligd. Mede hierom besloot de AP onderzoek te doen.

Conclusie

De AP constateert dat een aantal aangekondigde verbetermaatregelen zijn getroffen waardoor het risico op datalekken is verminderd. Wel ziet de AP nog wezenlijke risico's voor de beveiliging van persoonsgegevens die aanvullende verbetermaatregelen vereisen. Het gaat hier in het bijzonder om risico's die verband houden met het grote aantal partijen dat betrokken is bij de verwerkingen van persoonsgegevens in verband met het testen, vaccineren en bron- en contactonderzoek. In ieder geval zijn dit de 25 regionale GGD'en, de landelijke koepelorganisatie GGD GHOR, zes landelijke partnerorganisaties (callcenters en alarmcentrales)[1], diverse uitzendbureaus en IT-leveranciers. Duidelijke afspraken tussen de betrokken organisaties over bepaalde beveiligingsaspecten rondom de systemen die voor bron- en contactonderzoek worden gebruikt ontbreken. Dit geldt bijvoorbeeld ten aanzien van het autorisatiebeheer en de controle van logbestanden. Hierdoor is onvoldoende duidelijk wie waarvoor verantwoordelijk is en wie welke maatregelen in dit verband dient te treffen. Dat vergroot de kans op nieuwe tekortkomingen in de beveiliging van persoonsgegevens.

Verder werken het ministerie van Volksgezondheid, Welzijn en Sport, GGD GHOR en de GGD'en aan het vervangen van de systemen voor bron- en contactonderzoek (HPZone en HPZone Lite). In dit kader merkt de AP op dat vervanging van een systeem niet zonder meer leidt tot een betere beveiliging van de persoonsgegevens die daarin worden verwerkt. Hierbij wil de AP benadrukken dat bij de ontwikkeling en implementatie van een nieuw systeem nadrukkelijk rekening moet worden gehouden met de uit de Algemene verordening gegevensbescherming (hierna: AVG) voortvloeiende verplichtingen, zoals het vroegtijdig uitvoeren van een risicoanalyse in de vorm van een gegevensbeschermingseffectbeoordeling (artikel 35 AVG), de toepassing van gegevensbescherming door ontwerp en door standaardinstellingen (artikel 25 AVG) en het treffen van passende technische en organisatorische maatregelen ter beveiliging van persoonsgegevens (artikel 32 AVG), zoals bijvoorbeeld logging, controle op de logging en autorisatiebeheer.

Onderzoek

De AP heeft in het bijzonder onderzocht of voldoende verbetermaatregelen zijn getroffen met het oog op toegangsbeveiliging, verleende autorisaties en autorisatiebeheer, logging van de gebruikte systemen, controle op deze logging en om het ongeoorloofd exporteren/printen van persoonsgegevens uit de systemen te voorkomen. Ook heeft de AP gecontroleerd of de aangekondigde maatregelen met betrekking tot beperking van de zoekfuncties van gebruikers in de systemen ook daadwerkelijk zijn getroffen. Daarnaast is onderzocht of de betrokkenen die geraakt zijn door het datalek in overeenstemming met de

[1] Met de landelijke partners of partnerorganisaties worden bedoeld de callcenters en andere externe organisaties die worden ingezet om bron- en contactonderzoek uit te voeren en test- en vaccinatieafspraken te maken.

AVG zijn geïnformeerd over de inbreuk in verband met hun persoonsgegevens. Tenslotte heeft de AP – naar aanleiding van nieuwe zorgelijke berichtgeving in de media in februari 2021 – onderzocht of de website www.coronatest.nl aan de beveiligingseisen voldoet die gelden voor aansluiting op DigiD.

Het onderzoek was gericht op de systemen die worden gebruikt voor het verwerken van persoonsgegevens in het kader van de coronapandemie, namelijk voor het testen en vaccineren (CoronIT) en bron- en contractonderzoek (HPZone en HPZone Lite).

In het kader van het onderzoek heeft de AP controles uitgevoerd bij GGD GHOR en steekproefsgewijs bij twee regionale GGD'en en een van de landelijke partners die capaciteit leveren voor het uitvoeren van bron- en contactonderzoek. Onderstaande bevindingen zijn gebaseerd op de informatie die de AP tijdens het onderzoek heeft verzameld.

Bevindingen

1. Ter inleiding

Artikel 5, eerste lid, onderdeel f, AVG bevat het beginsel van vertrouwelijkheid en integriteit van persoonsgegevens. Door het nemen van passende technische en organisatorische maatregelen moeten persoonsgegevens op zodanige manier worden verwerkt dat een passende beveiliging ervan is gewaarborgd en dat zij onder meer zijn beschermd tegen ongeoorloofde of onrechtmatige verwerking. Artikel 32, eerste lid, AVG werkt dit beginsel uit en verplicht de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen te treffen om een op het risico voor betrokkene afgestemd beveiligingsniveau te waarborgen. Hierbij houdt de verwerkingsverantwoordelijke rekening met de beschikbare technologie en de uitvoeringskosten en met de aard, omvang, context en doeleinden van de verwerking. Wanneer sprake is van verwerking van informatie in zorginformatiesystemen dient de verwerkingsverantwoordelijke bij de invulling van deze verplichting voorts rekening te houden met de Nederlandse normen voor informatiebeveiliging in de zorg (NEN7510, 7512 en 7513).[2]

2. Toegangsbeveiliging

Onderdeel van de beveiliging van persoonsgegevens en het waarborgen van een passend beschermingsniveau vormt het voorkomen van ongeoorloofde toegang en implementeren van een authenticatieproces. Dit laatste betreft het proces waarbij een gebruiker van een computer of applicatie de geclaimde identiteit moet bewijzen. Tweefactorauthenticatie is een beveiligingsmaatregel in het authenticatieproces waarbij de gebruiker zich met een combinatie van twee verschillende typen authenticatiefactoren moet authenticeren om toegang te krijgen tot bijvoorbeeld een systeem. Dit verhoogt de zekerheid dat de gebruiker is wie hij zegt dat hij is.

[2] Zie ook artikel 3 en 5 Besluit elektronische gegevensverwerking door zorgaanbieders.

De AP heeft geconstateerd dat de drie onderzochte systemen vanaf eigen apparatuur rechtstreeks kunnen worden benaderd via een URL en dus zonder dat vereist is om eerst te zijn ingelogd op een beveiligde werkomgeving. Bij het verkrijgen van toegang tot de drie onderzochte systemen wordt wel tweefactorauthenticatie toegepast.

Uit het onderzoek is voorts gebleken dat de twee onderzochte GGD'en laptops verstrekken aan een deel van hun medewerkers. Uit het onderzoek blijkt echter ook dat een grote groep medewerkers, waaronder medewerkers van de landelijke partners, op eigen apparatuur werkt. Hiervoor is geen eenduidig beleid aangetroffen. Daarnaast heeft de GGD GHOR aangegeven met de landelijke partners geen afspraken te hebben vastgelegd over het werken op eigen apparatuur.

De AP merkt op dat het gebruik van eigen apparatuur in combinatie met de mogelijkheid om op de onderzochte systemen in te loggen buiten een beveiligde werkomgeving, kan leiden tot beveiligingsrisico's. Dit houdt verband met het feit dat de eigen apparatuur niet in beheer is bij de werkgever. Hierdoor is niet bekend of de apparatuur aan bepaalde beveiligingseisen voldoet en is het niet mogelijk om bepaalde technische beveiligingsmaatregelen, zoals het uitvoeren van noodzakelijke beveiligingsupdates, op de apparatuur af te dwingen. Ook bestaat het risico dat software op de apparatuur wordt geïnstalleerd die risico's voor de bescherming van persoonsgegevens met zich meebrengt. Dit kan deze apparatuur bijvoorbeeld kwetsbaarder maken voor aanvallen van buitenaf. Een mitigerende maatregel voor de risico's van werken op eigen apparatuur kan zijn ervoor zorg te dragen dat uitsluitend toegang tot de systemen kan worden verkregen binnen een beveiligde werkomgeving. Het feit dat via een internetbrowser en dus ook buiten een beveiligde werkomgeving kan worden ingelogd op de onderzochte systemen, kan dan ook, zoals gezegd, tot beveiligingsrisico's leiden. Op deze wijze kunnen immers de in de beveiligde werkomgeving genomen beveiligingsmaatregelen worden omzeild.

Met inachtneming van deze risico's, dienen GGD GHOR en de GGD'en passende beveiligingsmaatregelen te nemen en beleid vast te stellen dat is afgestemd op de risico's voor betrokkenen. De AP draagt GGD GHOR en de GGD'en op per direct dergelijke maatregelen te onderzoeken en vervolgens te implementeren én beleid vast te stellen over het gebruik van eigen apparatuur. De AP verwacht in een voortgangsrapportage (zie onder paragraaf 9) een terugkoppeling van de verbetermaatregelen die in dit verband zijn of worden getroffen.

3. Autorisaties

Autorisatie is het proces waarin een persoon bepaalde aan hem of haar toegekende rechten krijgt binnen een systeem. Autorisaties en het juiste beheer daarvan, zoals het tijdige aanpassen of intrekken van een autorisatie, kunnen bijdragen aan een passend beveiligingsbeleid binnen een organisatie. Het doel hiervan is dat medewerkers enkel toegang hebben tot persoonsgegevens of functionaliteiten die noodzakelijk zijn voor de uitvoering van hun werk.

De AP concludeert dat het proces rond het tijdig aanpassen of intrekken van autorisaties nog niet altijd goed verloopt. Duidelijke afspraken tussen de betrokken partijen hierover zijn niet aangetroffen. Het

autorisatieproces tot HPZone en HPZone Lite is in principe decentraal bij de GGD'en belegd. Elke GGD verzorgt zelf de toegang tot deze systemen en kent rollen toe aan eigen en ingehuurde medewerkers. Voor de medewerkers die door landelijke partners (callcenters en alarmcentrales) worden ingezet ter ondersteuning van de GGD'en bij het bron- en contactonderzoek, verloopt het autorisatieproces iets anders. Zij krijgen eerst door de landelijke partner de rollen toegekend die nodig zijn voor hun werkzaamheden en krijgen daarmee toegang tot het systeem HPZone (Lite), maar nog niet tot de gegevens daarin. Vervolgens verleent de GGD waarvoor de desbetreffende medewerker gaat werken toegang tot de regionale gegevens van die GGD. Deze medewerker heeft daarna alleen toegang tot de gegevens in HPZone (Lite) van personen in de regio van de betreffende GGD. Wanneer de medewerker van de landelijke partner vervolgens bij een andere GGD wordt ingezet, dient de landelijke partner de desbetreffende GGD te verzoeken om de toegang tot de regionale gegevens weer in te trekken.

Uit controles die de twee onderzochte GGD'en hebben uitgevoerd na het datalek van januari 2021 bleek dat diverse medewerkers over autorisaties beschikten die zij voor hun werkzaamheden niet of niet langer nodig hadden. Naar aanleiding van deze controles hebben de twee onderzochte GGD'en de niet-noodzakelijke autorisaties ingetrokken. Door de onderzochte GGD'en is aangegeven dat zij niet altijd informatie van de landelijke partners ontvingen over gewijzigde werkzaamheden van medewerkers uit deze flexibele landelijke schil. De AP heeft tijdens het onderzoek geen duidelijke gedocumenteerde afspraken tussen de betrokken partijen aangetroffen, die zijn opgesteld naar aanleiding van het datalek in januari 2021, voor het toewijzen, wijzigen en intrekken van autorisaties.

Daarnaast heeft de AP geen toereikende documentatie aangetroffen die ten aanzien van HPZone en HPZone Lite inzichtelijk maakt welke specifieke rechten en functionaliteiten aan de verschillende rollen in de autorisatiematrix zijn gekoppeld.

Tegen deze achtergrond draagt de AP GGD GHOR en de GGD'en op om duidelijke afspraken te maken met de betrokken partijen met betrekking tot het autorisatieproces en de procedures eenduidig vast te leggen. Dit betreft zowel de huidige systemen zolang deze nog in gebruik zijn voor de bestrijding van de coronapandemie als de vervangende systemen wanneer deze in productie worden genomen. Voorts dienen GGD GHOR en de GGD'en de verleende autorisaties regelmatig te (blijven) beoordelen en ook hiervoor duidelijke afspraken te maken wie in dit verband welke acties dient te verrichten. De AP verwacht in een voortgangsrapportage een terugkoppeling van de verbetermaatregelen die in dit verband zijn of worden getroffen.

4. Logging en controle op de logging

Logging is het proces waarbij systeemactiviteiten, bijvoorbeeld bepaalde handelingen van een gebruiker in een systeem, worden vastgelegd in logbestanden. Het vastleggen van gebeurtenissen in logbestanden en regelmatige controle daarvan vormt een belangrijk onderdeel van informatiebeveiliging. Aan de hand van de logbestanden kan worden nagegaan wie bepaalde gegevens heeft bekeken of aangepast. Ook kunnen uit logbestanden pogingen om ongeautoriseerd toegang te krijgen worden geïdentificeerd. Op basis van de

verkregen loginformatie kan efficiënter in actie worden gekomen bij een datalek en/of worden bepaald of aanvullende technische en organisatorische maatregelen nodig zijn.

Uit het onderzoek van de AP is gebleken dat op alle drie de onderzochte systemen logbestanden werden en nog steeds worden gemaakt van gebeurtenissen die in die systemen plaatsvinden, maar dat de logbestanden voorafgaand aan het datalek van januari 2021 niet regelmatig werden gecontroleerd. De logbestanden van CoronIT werden enkel naar aanleiding van een incident of klacht gecontroleerd door de GGD GHOR. Of de logbestanden van HPZone en HPZone Lite werden gecontroleerd en zo ja, door wie, heeft de AP niet kunnen vaststellen.

In september 2020 heeft GGD GHOR, in antwoord op vragen van de AP naar aanleiding van een eerdere datalekmelding, aangegeven dat in het vierde kwartaal van 2020 geautomatiseerde controle van de logbestanden zou worden ingericht. Op basis van deze informatie besloot de AP destijds de datalekmelding af te sluiten. In januari 2021 bleek deze geautomatiseerde controle nog niet te zijn ingericht. Na het datalek van januari 2021 gaf GGD GHOR aan de geautomatiseerde controle in de vorm van SIEM-oplossing (*Security Information & Event Management*) versneld te zullen implementeren; deze zou eind maart 2021 gereed zijn. Ook deze planning is niet gehaald. De AP constateert dat de SIEM-oplossing in ieder geval ten tijde van het afronden van de onderzoeksfase in juni 2021 nog steeds niet was geïmplementeerd.

Als mitigerende en alternatieve maatregel heeft GGD GHOR, naar aanleiding van het datalek van januari 2021 en in afwachting van de SIEM-oplossing, dagelijkse handmatige controle van de logbestanden van alle drie de systemen ingericht. Deze controles worden met behulp van queries uitgevoerd door een team bij het Security Operations Center (SOC) van GGD GHOR. Dit gebeurt op basis van bepaalde criteria en procedures met het doel om afwijkende gebeurtenissen vast te stellen. In het kader van de SIEM-oplossing werkt het SOC in samenwerking met twee externe partijen aan relevante *use cases* en *business rules* op basis van de kennis opgedaan bij de handmatige controle van de logbestanden van CoronIT, HPZone en HPZone Lite, ten einde bepaalde onregelmatigheden vooraf te definiëren waarop automatisch kan worden gemonitord.

Met het oog op de aanstaande vervanging van de systemen HPZone en HPZone Lite, benadrukt de AP dat GGD GHOR en de GGD'en bij het in productie nemen van vervangende systemen van meet af aan de logging en de controle op de logging goed moeten inrichten zodat regelmatige controle van de logbestanden is verzekerd. De AP verwacht in een voortgangsrapportage een terugkoppeling van de maatregelen die in dit verband zijn of worden getroffen.

5. Export- en printfunctionaliteiten

Export- en printfunctionaliteiten maken het onder andere mogelijk om (lijsten met) persoonsgegevens gemakkelijk uit een systeem te halen. Door deze functionaliteiten alleen toe te kennen aan gebruikers die deze ook nodig hebben voor hun werkzaamheden, kan het risico op misbruik van persoonsgegevens worden verkleind.

De AP heeft vastgesteld dat naar aanleiding van het datalek van januari 2021 deze functionaliteiten in de drie onderzochte systemen zijn uitgeschakeld respectievelijk zijn teruggebracht tot een selecte groep gebruikers die deze nodig hebben voor hun werkzaamheden.

Voor CoronIT geldt dat de functionaliteit voor het uitprinten van afsprakenlijsten met persoonsgegevens kort na het datalek van januari 2021 is uitgeschakeld. Voor HPZone en HPZone Lite geldt dat de export- en printfunctie in HPZone is beperkt tot twee rollen en in HPZone Lite tot één rol. Deze rollen zijn aan een selecte groep van medewerkers toebedeeld die deze functionaliteit nodig hebben voor de uitvoering van hun werkzaamheden.

In het licht van de aanstaande vervanging van HPZone en HPZone Lite, benadrukt de AP dat reeds bij de ontwikkeling en implementatie van een nieuw systeem secuur moet worden gekeken naar welke gebruikers welke functionaliteiten nodig hebben en dat autorisaties daarmee in lijn moeten worden gebracht. De AP verwacht in een voortgangsrapportage een terugkoppeling van de verbetermaatregelen die in dit verband zijn of worden getroffen.

6. Zoekfunctionaliteiten

Door zoekfunctionaliteiten in een systeem te beperken, kan het risico dat onbevoegd persoonsgegevens van een specifieke persoon, bijvoorbeeld van een bekende Nederlander, worden opgezocht en ingezien, worden verminderd. Dit kan bijvoorbeeld door de zoekfunctionaliteit zodanig in te stellen dat het niet mogelijk is om de gegevens van een specifieke persoon op te zoeken aan de hand van algemeen bekende of gemakkelijk op te zoeken kenmerken.

De AP heeft geconstateerd dat naar aanleiding van het datalek in januari 2021 in CoronIT de zoekfunctionaliteit is aangepast. Hierdoor is het niet meer mogelijk om enkel op achternaam of een combinatie van achternaam en geslacht of achternaam en geboortedatum de gegevens van een specifieke persoon in dit systeem op te zoeken. Uit het onderzoek van de AP blijkt echter dat een vergelijkbare beperking van de zoekfunctionaliteit in HPZone en HPZone Lite niet is aangebracht, volgens GGD GHOR vanwege technische beperkingen bij de leveranciers. Wel zijn maatregelen getroffen om ervoor te zorgen dat in het resultaat van een zoekopdracht minder persoonsgegevens zichtbaar zijn.

In het kader van het besluit de systemen HPZone en HPZone Lite te vervangen, wijst de AP GGD GHOR en de GGD'en nadrukkelijk op het feit dat bij de ontwikkeling en implementatie van een of meer nieuwe systemen, ook aandacht moet worden besteed aan de risico's voor de bescherming van persoonsgegevens die gepaard kunnen gaan met een ruime zoekfunctionaliteit. De AP verwacht in een voortgangsrapportage een terugkoppeling van de maatregelen die in dit verband zijn of worden getroffen.

7. Beveiligingseisen voor aansluiting DigiD

De AP concludeert dat GGD GHOR ten aanzien van de website www.coronatest.nl op dit moment voldoet aan de normen die voortvloeien uit de “Norm ICT-beveiligingsassessments DigiD”.

Ter toelichting geldt het volgende. Ten tijde van het lopende onderzoek verscheen in de media zorgelijke berichtgeving over de aansluiting van www.coronatest.nl op DigiD. Omdat niet aan alle beveiligingseisen zou zijn voldaan, bestond het risico dat www.coronatest.nl de aansluiting op DigiD zou verliezen. Gelet op het feit dat hierdoor mogelijk sprake was van een risico voor de bescherming van persoonsgegevens die via deze website werden verwerkt, besloot de AP de reikwijdte van het onderzoek uit te breiden en te monitoren of noodzakelijke verbetermaatregelen door GGD GHOR werden getroffen. Op basis van de beschikbare informatie heeft de AP kunnen concluderen dat GGD GHOR ten aanzien van www.coronatest.nl op dit moment voldoet aan de normen die voortvloeien uit de “Norm ICT-beveiligingsassessments DigiD”.

8. Informeren van betrokkenen

Indien zich een datalek heeft voorgedaan dat waarschijnlijk een hoog risico voor de rechten en vrijheden van betrokkenen inhoudt, dient aan de betrokkenen hiervan onverwijld mededeling te worden gedaan, tenzij sprake is van een in artikel 34 AVG genoemde uitzondering. De mededeling moet in ieder geval de in artikel 34 AVG genoemde informatie te bevatten. Het belangrijkste doel daarvan is dat betrokkenen begrijpen wat er met hun persoonsgegevens is gebeurd en wat zij kunnen doen om zichzelf te beschermen.

Naar aanleiding van de datalekmelding bij de AP op 22 januari 2021, is er tussen 25 januari en 29 januari 2021 meermaals contact geweest tussen de AP en GGD GHOR over de kennisgeving richting betrokkenen op grond van artikel 34 AVG. De AP heeft geconstateerd dat GGD GHOR op 29 januari 2021 op haar website informatie aan betrokkenen heeft verstrekt over het datalek. Op 16 maart 2021 is voorts een aantal geïdentificeerde betrokkenen per brief geïnformeerd over het datalek. De informatie die aan betrokkenen is verstrekt omvatte de waarschijnlijke gevolgen van het datalek en maatregelen die zijn voorgesteld of genomen om het datalek aan te pakken en nadelige gevolgen te beperken. Betrokkenen zijn alert gemaakt op de mogelijke gevolgen van het datalek, waardoor zij zich hiertegen, voor zover dat mogelijk is, kunnen wapenen door bijvoorbeeld extra voorzorgsmaatregelen te treffen. Ook is informatie over een contactpunt verstrekt, waar betrokkenen meer informatie kunnen verkrijgen. De AP begrijpt dat het politieonderzoek dat naar aanleiding van het datalek is gestart nog loopt. Indien uit dit onderzoek nieuwe betrokkenen worden geïdentificeerd die geraakt zijn door het datalek, wijst de AP GGD GHOR en de GGD’en op de verplichting deze personen te informeren op vergelijkbare wijze waarop GGD GHOR, al dan niet in opdracht van de GGD’en, de eerder geïdentificeerde betrokkenen heeft geïnformeerd.

9. Ten slotte

Uit het onderzoek van de AP is gebleken dat een groot aantal partijen betrokken is bij de verwerking van persoonsgegevens in de drie onderzochte systemen. In de eerste plaats betreft dit de 25 regionale GGD’en.

Datum
8 november 2021

Ons kenmerk
z2021-02000

Er bestaat in Nederland niet één GGD-organisatie. Er is een landelijk dekkend netwerk van 25 gemeentelijke gezondheidsdiensten (GGD'en). Dit zijn 25 afzonderlijke publiekrechtelijke rechtspersonen. Iedere GGD wordt aangestuurd door een eigen Directeur Publieke Gezondheid in de desbetreffende regio. Daarnaast bestaat GGD GHOR Nederland (GGD GHOR). GGD GHOR is de overkoepelende brancheorganisatie van de 25 regionale GGD'en en behartigt de belangen van de publieke gezondheid en veiligheid in Nederland. Ten behoeve van de werkzaamheden die de 25 GGD'en in het kader van de coronapandemie moesten verrichten (testen, vaccineren en bron- en contactonderzoek), heeft GGD GHOR een aantal zaken centraal op zich genomen. Dit betreft onder andere het laten ontwikkelen van applicaties die door alle 25 GGD'en worden gebruikt, zoals CoronIT en HP Zone Lite en het sluiten van overeenkomsten met landelijke partnerorganisaties die werkzaamheden voor de GGD'en verrichten zoals het maken van test- en vaccinatieafspraken en het uitvoeren van bron- en contactonderzoek.

Naast de 25 GGD'en en GGD GHOR zijn in ieder geval zes landelijke partnerorganisaties (callcenters en alarmcentrales) en de IT-leveranciers van de systemen betrokken bij de verwerking van persoonsgegevens in het kader van het testen, vaccineren en bron- en contactonderzoek. De landelijke partners en de GGD'en huren op hun beurt weer tijdelijk personeel in bij diverse uitzendbureaus.

De AP draagt GGD GHOR en de GGD'en op om onderling en met de overige betrokken partijen per direct duidelijke afspraken op het vlak van informatiebeveiliging te maken, vast te leggen en actueel te houden. Voor partijen dient duidelijk te zijn wie voor welke technische en/of organisatorische maatregelen verantwoordelijk is. Dat is nu onvoldoende geregeld. Uit de gesprekken is namelijk het beeld naar voren gekomen dat met name ten aanzien van HPZone Lite onduidelijkheid bestaat over de verantwoordelijkheidsverdeling. Voor zover sprake is van gezamenlijke verwerkingsverantwoordelijkheid, wijst de AP op artikel 26, eerste lid, AVG dat vereist dat partijen in een onderlinge regeling op transparante wijze hun respectievelijke verantwoordelijkheden voor naleving van de AVG vastleggen.

De AP verwacht in een voortgangsrapportage hierop een reactie en een overzicht van de verbetermaatregelen die in dit verband zijn of worden getroffen.

Ter afsluiting

De AP heeft onderzoek gedaan bij GGD GHOR en twee (regionale) GGD'en naar de beveiliging van persoonsgegevens die in het kader van de coronapandemie. worden verwerkt in CoronIT, HPZone en HPZone Lite. Deze systemen worden door alle 25 GGD'en gebruikt en de beveiliging van de daarin verwerkte persoonsgegevens is dus mede afhankelijk van maatregelen die alle 25 GGD'en afzonderlijk dan wel gezamenlijk treffen om de persoonsgegevens passend te beveiligen. De bevindingen van de AP zijn dan ook relevant voor alle 25 GGD'en. De AP verwacht daarom dat alle GGD'en de in deze brief genoemde noodzakelijke verbetermaatregelen - voor zover zij dat nog niet hebben gedaan - zullen treffen om een passend niveau van beveiliging van persoonsgegevens te waarborgen. Mede met het oog hierop zal deze brief ook aan de overige 23 GGD'en worden gezonden.

Datum
8 november 2021

Ons kenmerk
z2021-02000

Informatiebeveiliging is een continu proces waarin risico's en maatregelen periodiek moeten worden (her)beoordeeld zodat de technische en organisatorische beveiligingsmaatregelen steeds zijn afgestemd op de actuele risico's voor betrokkenen. Om deze reden benadrukt de AP met klem het belang om audits gericht op informatiebeveiliging te blijven uitvoeren en risico's en maatregelen periodiek te (her)beoordelen zodat, waar nodig, (aanvullende) technische en organisatorische maatregelen ter beveiliging van de (bijzondere) persoonsgegevens die worden verwerkt tijdig kunnen worden genomen.

De AP heeft inmiddels de bevindingen van het onderzoek in een gesprek aan GGD GHOR toegelicht en zal erop toezien dat noodzakelijke verbeteringen tijdig worden doorgevoerd. De AP verzoekt GGD GHOR dan ook om uiterlijk op 1 maart 2022 in een voortgangsrapportage op elk van de in deze brief aangegeven punten aan te geven welke verbetermaatregelen daadwerkelijk zijn of worden getroffen om de geïdentificeerde risico's ten aanzien van de beveiliging van persoonsgegevens die worden verwerkt in het kader van de coronapandemie te verminderen. Dit betreft zowel de huidige systemen zolang deze nog worden gebruikt voor de bestrijding van de coronapandemie als de vervangende systemen wanneer deze in productie worden genomen. Mocht de in de voortgangsrapportage genoemde implementatie van verbetermaatregelen onverhoopt vertraging oplopen, dan verwacht de AP daarover door GGD GHOR onverwijld te worden geïnformeerd.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd. Voor eventuele vragen kunt u contact opnemen met bovengenoemd contactpersoon.

Een afschrift van deze brief zend ik aan de functionaris voor de gegevensbescherming van uw organisatie.

Hoogachtend,
Autoriteit Persoonsgegevens,

w.g.

ir. M.J. Verdier
Vicevoorzitter