AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Hoge Nieuwstraat 8, 2514 EL Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

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

Datum	Ons kenmerk	Uw brief van
29 september 2022	z2021-02000	28 februari 2022

Contactpersoon
[...]

Afronding onderzoek GGD GHOR en twee GGD'en

Geachte heer Rouvoet,

Bij brief van 8 november 2021 (hierna: de eindbrief) heeft de Autoriteit Persoonsgegevens (hierna: AP) u geïnformeerd over de bevindingen voortvloeiend uit haar onderzoek bij GGD GHOR Nederland (hierna: GGD GHOR) en twee regionale GGD'en. Aanleiding voor dat onderzoek vormden het in januari 2021 door GGD GHOR mede namens de regionale GGD'en aan de AP gemelde datalek, zorgwekkende berichtgeving in de media over de diefstal van persoonsgegevens en de bezorgde signalen die de AP hierover ontving.[1]

Kort gezegd constateerde de AP dat een aantal verbetermaatregelen waren getroffen ter beveiliging van persoonsgegevens die worden verwerkt in het kader van de coronapandemie in de onderzochte systemen (CoronIT, HPZone en HPZone Lite). Daardoor verminderde het risico op datalekken. Wel zag de AP nog wezenlijke risico's voor de beveiliging van persoonsgegevens die om aanvullende verbetermaatregelen vroegen. Zo vereist het grote aantal organisaties dat betrokken is bij de verwerking van persoonsgegevens in het kader van coronapandemie dat duidelijke afspraken worden gemaakt over de beveiliging van die persoonsgegevens. De AP constateerde dat er op bepaalde vlakken, waaronder autorisatiebeheer, onduidelijkheid bestond wie welke maatregelen moest treffen. Ook wees de AP op de beveiligingsrisico's die gepaard kunnen gaan met het gebruik van eigen apparatuur[2] in combinatie met de mogelijkheid om op de onderzochte coronasystemen in te loggen buiten een beveiligde werkomgeving.

[1] De eindbrief is gepubliceerd op de website van de AP (https://autoriteitpersoonsgegevens.nl/nl/nieuws/ggd-moet-persoonsgegevens-beter-beschermen).
[2] Ook wel aangeduid met BYOD - Bring Your Own Device.

Datum
29 september 2022

Ons kenmerk
z2021-02000

De AP heeft GGD GHOR in de eindbrief verzocht om uiterlijk op 1 maart 2022 in een voortgangsrapportage aan te geven welke aanvullende verbetermaatregelen zijn of worden getroffen om de in de brief geïdentificeerde risico's te verminderen, zowel ten aanzien van de huidige systemen als ten aanzien van vervangende systemen wanneer deze in productie worden genomen.

Op 28 februari jl. ontving de AP van GGD GHOR drie voortgangsrapportages: één van GGD GHOR en één van ieder van de twee onderzochte regionale GGD'en, alle voorzien van een aantal bijlagen. De AP heeft deze voortgangsrapportages met bijlagen beoordeeld en komt tot de volgende conclusie.

Conclusie

Op basis van de in de voortgangsrapportages verstrekte informatie in samenhang met de bevindingen van de AP zoals beschreven in de eindbrief van 8 november 2021, concludeert de AP dat er op dit moment geen aanleiding is om verder onderzoek te doen bij GGD GHOR en de twee onderzochte GGD'en naar de beveiliging van persoonsgegevens die worden verwerkt met het oog op het testen, vaccineren en het uitvoeren van bron- en contactonderzoek in verband met de coronapandemie in de drie onderzochte systemen. De AP rondt daarmee haar onderzoek naar de drie organisaties af.
Dit laat onverlet dat de beveiliging van persoonsgegevens géén eenmalige exercitie is, maar een doorlopend proces. Daarom benadrukt de AP dat onder de AVG verwerkingsverantwoordelijken en verwerkers, waar passend, een procedure moeten hebben voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking, teneinde een op het risico afgestemd beveiligingsniveau blijvend te waarborgen. Mocht daartoe aanleiding bestaan, dan kan de AP opnieuw een onderzoek starten en, bij constatering van overtreding van de AVG, handhavend optreden.

Aandachtspunten voortvloeiend uit de voortgangsrapportages

Lezing van de ontvangen voortgangsrapportages geeft de AP aanleiding om voor de volgende drie punten extra aandacht te vragen.

A. Zorg dat afspraken over informatiebeveiliging tussen de betrokken partijen actueel blijven en herzie deze indien daartoe aanleiding is.
B. Zorg ervoor dat bij het in gebruik nemen van GGD Contact alle essentiële beveiligingsmaatregelen waaronder regelmatige controle van de logbestanden van meet af aan op orde zijn.
C. Maak vaart met het opzetten van de beveiligde digitale werkomgeving voor toegang tot corona-applicaties.

Ad A. Zorgdragen voor duidelijke afspraken tussen betrokken partijen over informatiebeveiliging

De AP heeft in haar eindbrief geconstateerd dat een groot aantal verschillende partijen samenwerken bij de verwerking van persoonsgegevens in de onderzochte systemen. Naast de 25 GGD'en waren dit onder andere zes landelijke partners die werden en deels worden ingezet bij de coronabestrijding. GGD GHOR heeft voorts meermaals benadrukt dat de 25 GGD'en alle zelfstandige publiekrechtelijke rechtspersonen zijn met ieder een eigen verantwoordelijkheid voor het treffen van passende beveiligingsmaatregelen. Om een passend beveiligingsniveau te waarborgen van de persoonsgegevens die alle partijen samen verwerken in de coronasystemen, zijn onderlinge afspraken op het vlak van informatiebeveiliging onmisbaar. Van belang hierbij is dat deze afspraken voor alle partijen duidelijk zijn, worden vastgelegd en actueel worden gehouden.

Uit de voortgangsrapportages blijkt dat verbeteringen hebben plaatsgevonden. GGD GHOR heeft aangegeven dat het aantal landelijke partners is teruggebracht en met deze landelijke partners afspraken zijn gemaakt ten aanzien van de bescherming en het verwerken van persoonsgegevens, waaronder het implementeren van technische en organisatorische beveiligingsmaatregelen. Ten aanzien van het intrekken en wijzigen van autorisaties, zijn volgens GGD GHOR sluitende en controleerbare afspraken gemaakt met de landelijke partners. Verder hebben GGD GHOR en de 25 GGD'en als gezamenlijke verwerkingsverantwoordelijken twee convenanten gesloten met betrekking tot de verwerking van persoonsgegevens in de systemen CoronIT en in HPZone (Lite). Ten aanzien van GGD Contact heeft GGD GHOR aangegeven een verwerkersovereenkomst te hebben gesloten met de 25 GGD'en waarbij de GGD'en als verwerkingsverantwoordelijken zijn aangemerkt en GGD GHOR als verwerker.

De AP benadrukt nogmaals het belang van dergelijke afspraken. Het gaat daarbij ook om het actueel houden van de gemaakte afspraken en deze zo nodig te herzien wanneer de ontwikkelingen daartoe aanleiding geven. Voor partijen moet steeds duidelijk zijn (per systeem of applicatie) wie voor welke technische en/of organisatorische maatregelen verantwoordelijk is, zodat de noodzakelijk te nemen maatregelen niet tussen wal en schip vallen waardoor de belangen van betrokkenen kunnen worden geschaad.

Ad. B Beveiligingsmaatregelen treffen met betrekking tot GGD Contact

In haar eindbrief heeft de AP beschreven dat het ministerie van Volksgezondheid, Welzijn en Sport (hierna: ministerie van VWS), GGD GHOR en de GGD'en werken aan het vervangen van de systemen voor bron- en contactonderzoek (HPZone en HPZone Lite). De applicatie GGD Contact zal in ieder geval HPZone Lite gaan vervangen. De AP merkte eerder al op dat vervanging van een systeem niet automatisch leidt tot een betere beveiliging van de persoonsgegevens die daarin worden verwerkt. Zij benadrukte daarbij dat bij de ontwikkeling en implementatie van een nieuw systeem nadrukkelijk rekening moet worden gehouden met de uit de AVG voortvloeiende verplichtingen, waaronder het treffen van passende technische en organisatorische maatregelen ter beveiliging van persoonsgegevens, zoals bijvoorbeeld logging, controle op de logging en autorisatiebeheer.

GGD GHOR geeft in haar voortgangsrapportage aan dat GGD Contact deels al in gebruik is bij GGD'en en een landelijke partner. Ten aanzien van de logging en controle op de logging, geeft GGD GHOR aan dat het ministerie van VWS heeft bepaald welk gedrag als afwijkend moet worden beschouwd. Ook heeft het ministerie van VWS GGD GHOR de mogelijkheid gegeven om dat gedrag te monitoren. In de nabije toekomst, zo geeft GGD GHOR aan, zullen de loggegevens van GGD Contact worden 'ingelezen' in de SIEM-oplossing (Security Information & Event Management). Hierdoor kunnen deze loggegevens geautomatiseerd worden gecontroleerd en is geen handmatige controle nodig. De AP gaat ervan uit dat tot die tijd, GGD GHOR ervoor zorgdraagt dat periodieke controle van de logbestanden voldoende is geborgd.

In een van de bijlagen bij de voortgangsrapportage is uiteen gezet dat een veilig gebruik van GGD Contact om maatregelen binnen de eigen GGD vraagt. Van de GGD'en wordt verwacht dat ieder van hen onder andere een organisatie-eigen DPIA uitvoert en maatregelen implementeert. In samenspraak met de GGD'en is een inventarisatie gemaakt van de privacy- en informatiebeveiligingsmaatregelen om veilig met GGD Contact te werken. Op basis van die inventarisatie zijn adviezen geformuleerd waarmee de GGD'en nu zelf aan de slag kunnen. De AP wijst erop dat het belangrijk is dat de voorgestelde maatregelen daadwerkelijk worden getroffen en dat de adviezen door de GGD'en worden opgevolgd.

Ad. C Vaart maken met beveiligde digitale werkomgeving

De AP heeft in haar eindbrief geconstateerd dat voor de toegang tot de drie onderzochte coronasystemen tweefactorauthenticatie wordt toegepast. De AP heeft in de eindbrief echter tevens gewezen op de beveiligingsrisico's die gepaard kunnen gaan met het gebruik van eigen apparatuur van medewerkers (BYOD) in combinatie met de mogelijkheid om op de onderzochte coronasystemen in te loggen buiten een beveiligde werkomgeving. In dit verband heeft de AP in de eindbrief aangegeven dat de organisaties passende beveiligingsmaatregelen moeten nemen en beleid moeten vaststellen.

De AP heeft met instemming kennisgenomen van het feit dat GGD GHOR in haar voortgangsrapportage aangeeft een virtuele en beveiligde werkomgeving op te gaan zetten die volledig NEN7510, 7512 en 7513 compliant wordt ingericht. De corona-applicaties zullen alsdan alleen nog via deze beveiligde werkomgeving kunnen worden benaderd. De AP benadrukt dat dit een belangrijke beveiligingsmaatregel is en spoort GGD GHOR aan hiermee vaart te maken zodat deze werkomgeving voor alle betrokken partijen werkbaar is en zij hiervan gebruik kunnen gaan maken.

De twee onderzochte GGD'en geven in hun voortgangsrapportages aan dat zij maatregelen hebben genomen met betrekking tot het gebruik van eigen apparatuur. Zij geven voorts aan dat medewerkers de corona-applicaties alleen mogen benaderen via een beveiligde digitale werkomgeving. De AP spoort ook de andere GGD'en aan dit voorbeeld te volgen voor zover dat nog niet is gebeurd.

Datum
29 september 2022

Ons kenmerk
z2021-02000

Ter afsluiting

Tot slot wil de AP, óók richting de 23 GGD'en die zij niet in haar onderzoek heeft betrokken, nog het volgende benadrukken. Artikel 32 van de AVG vereist dat verwerkingsverantwoordelijken en verwerkers passende technische en organisatorische maatregelen treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. Dit veronderstelt dat verwerkingsverantwoordelijken en verwerkers op basis van een risicoanalyse zelf beoordelen welke maatregelen passend zijn. Zij moeten hierover verantwoording kunnen afleggen. Indien sprake is van verwerking van persoonlijke gezondheidsinformatie, vormen de Nederlandse normen voor informatiebeveiliging in de zorg (NEN7510, 7512 en 7513) hierbij een belangrijk ijkpunt .

Daarnaast bepaalt artikel 32 van de AVG dat, waar passend, een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking, onderdeel dient uit te maken van de maatregelen die moeten worden getroffen om een op het risico afgestemd beveiligingsniveau te waarborgen. Het periodiek (laten) uitvoeren van audits gericht op de evaluatie van technische en organisatorische beveiligingsmaatregelen (waarbij opvolging wordt gegeven aan de uitkomsten van deze audits en er een PDCA-cyclus tot stand komt), levert hieraan een waardevolle bijdrage.

De AP verwacht van GGD GHOR, de twee onderzochte GGD'en alsmede de 23 GGD'en die niet in het onderzoek zijn betrokken, dat zij de nodige maatregelen nemen en zullen blijven nemen om te borgen dat processen, procedures en (IT-)systemen nu en in de toekomst aan de vereisten van de AVG voldoen. Indien daartoe aanleiding bestaat, bijvoorbeeld omdat de AP opnieuw klachten of een datalekmelding ontvangt, kan de AP een nieuw onderzoek starten naar GGD GHOR en/of een of meer individuele GGD'en. Constateert de AP alsdan een overtreding van de AVG, dan kan dit leiden tot het opleggen van een boete of een maatregel.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd. Voor eventuele vragen kunt u contact opnemen met een van bovengenoemde contactpersonen.

Een afschrift van deze brief zend ik aan de functionaris voor gegevensbescherming van uw organisatie alsmede aan de 23 GGD'en die de AP niet in haar onderzoek heeft betrokken.

Hoogachtend,
Autoriteit Persoonsgegevens,

[w.g.]

ir. M.J. Verdier
Vicevoorzitter