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

Aangetekend
Stichting HagaZiekenhuis
[VERTROUWELIJK]
Postbus 40551
2504 LN DEN HAAG

Datum
18 juni 2019

Ons kenmerk
[VERTROUWELIJK]

Contactpersoon
[VERTROUWELIJK]

Onderwerp
Besluit tot het opleggen van een bestuurlijke boete en een last onder dwangsom

Geachte [VERTROUWELIJK],

De Autoriteit Persoonsgegevens (AP) heeft besloten aan Stichting HagaZiekenhuis (HagaZiekenhuis) een **bestuurlijke boete** van **€ 460.000,--** op te leggen, omdat het HagaZiekenhuis in de periode van januari 2018 tot heden niet heeft voldaan en niet voldoet aan het vereiste van tweefactor authenticatie en het regelmatig beoordelen van logbestanden. Daarmee heeft zij onvoldoende passende maatregelen genomen als bedoeld in artikel 32, eerste lid, van de Algemene Verordening Gegevensbescherming (AVG). De AP heeft tevens besloten aan het HagaZiekenhuis een **last onder dwangsom** op te leggen, die ziet op het ongedaan maken van deze voortdurende overtreding.

Hierna wordt het besluit nader toegelicht. Hoofdstuk 1 betreft een inleiding en Hoofdstuk 2 beschrijft het wettelijk kader. In Hoofdstuk 3 beoordeelt de AP haar bevoegdheid, de verwerkingsverantwoordelijkheid en de overtreding. In Hoofdstuk 4 wordt de (hoogte van de) bestuurlijke boete uitgewerkt en in Hoofdstuk 5 wordt de last onder dwangsom weergegeven. Hoofdstuk 6 bevat het dictum en de rechtsmiddelenclausule.

Datum
18 juni 2019

Ons kenmerk
[VERTROUWELIJK]

1. Inleiding

1.1 Betrokken rechtspersonen

Het HagaZiekenhuis betreft een stichting die statutair is gevestigd op de Els Borst-Eilersplein 275, (2545 AA) te Den Haag. Het HagaZiekenhuis is op 1 juli 2004 opgericht en is in het register van de Kamer van Koophandel ingeschreven onder nummer 27268552. In 2017 had het HagaZiekenhuis (afgerond) in totaal 28.500 opnamen, 158.000 eerste polikliniekbezoeken, 52.000 eerste hulp consulten en 143.000 verpleegdagen.[1]

Stichting Reinier Haga Groep (hierna: RHG) is statutair gevestigd op hetzelfde adres als het HagaZiekenhuis. RHG is op 12 juli 2013 opgericht en is in het register van de Kamer van Koophandel ingeschreven onder nummer 58365710. RHG wordt gevormd door Stichting Reinier de Graaf Groep, Stichting Langeland Ziekenhuis en het HagaZiekenhuis.

1.2 Procesverloop

Op 4 april 2018 heeft het HagaZiekenhuis een melding gedaan van een datalek aan de AP.[2] Het datalek had betrekking op onrechtmatige inzage in een patiëntendossier van een bekende Nederlander.

Naar aanleiding van die melding heeft de AP bij brief van 23 april 2018 een schriftelijk informatieverzoek verstuurd aan het HagaZiekenhuis. Hieraan heeft het HagaZiekenhuis bij brief van 15 mei 2018 gevolg gegeven.

De AP heeft naar aanleiding van de door het HagaZiekenhuis toegezonden informatie met toepassing van artikel 58, eerste lid, onder b, van de AVG besloten nader onderzoek te doen naar, voor zover hier van belang, de toegang tot patiëntgegevens in de digitale patiëntendossiers bij het HagaZiekenhuis. Bij brief van 12 oktober 2018 heeft de AP in dat kader een schriftelijk informatieverzoek verstuurd aan het HagaZiekenhuis. Hieraan heeft het HagaZiekenhuis gevolg gegeven.

Op 31 oktober 2018 heeft een aangekondigd onderzoek ter plaatse (hierna: OTP) bij het HagaZiekenhuis plaatsgevonden.

Bij brief van 19 november 2018 heeft de AP de zakelijke weergave van de betreffende verklaringen van de medewerkers van het HagaZiekenhuis tijdens het OTP aan het HagaZiekenhuis toegezonden met de mogelijkheid om de feitelijke (on)juistheid van de verklaringen kenbaar te maken.

Bij brief van 29 november 2018 heeft het HagaZiekenhuis haar opmerkingen op voornoemde verslagen kenbaar gemaakt.

[1] In dit kader verwijst de AP naar de door het HagaZiekenhuis ter zienswijzezitting overgelegde cijfers uit het Jaarverslag.
[2] Meldingsnummer [VERTROUWELIJK].

Het verslag van de gesprekken die tijdens het OTP plaatsvonden is - met inachtneming van de reactie van het HagaZiekenhuis op de zakelijke weergave van de verklaringen - op 19 december 2018 door de AP vastgesteld.

De resultaten van het nader onderzoek zijn vastgelegd in het rapport "Toegang tot digitale patiëntdossiers door medewerkers van het HagaZiekenhuis, Voorlopige bevindingen" van januari 2019 (hierna: rapport Voorlopige bevindingen).

Daartoe bij brief van 16 januari 2019 door de AP in de gelegenheid gesteld, heeft het HagaZiekenhuis bij brief van 4 februari 2019 haar reactie op het rapport Voorlopige bevindingen gegeven.

Met inachtneming van deze reactie heeft de AP het definitieve rapport vastgesteld. Dit rapport is bij brief van 26 maart 2019 aan het HagaZiekenhuis toegezonden.

Bij brief van 4 april 2019 heef de AP aan het HagaZiekenhuis een voornemen toegezonden tot het opleggen van een bestuurlijke boete en/of een last onder dwangsom wegens overtreding van artikel 32 van de AVG.

Daartoe tevens bij brief van 4 april 2019 door de AP in de gelegenheid gesteld, heeft het HagaZiekenhuis bij brief van 18 april 2019 schriftelijk haar zienswijze gegeven over dit voornemen en het daaraan ten grondslag gelegde definitieve rapport.

Op 25 april 2019 heeft ten kantore van de AP een zienswijzezitting plaatsgevonden waarbij het HagaZiekenhuis ook mondeling haar zienswijze heeft toegelicht.

Bij e-mail van 30 april 2019 heeft het HagaZiekenhuis desgevraagd twee stukken nagezonden.

Bij brief van 16 mei 2019 heeft de AP het verslag van de zienswijzezitting aan HagaZiekenhuis toegestuurd. Het HagaZiekenhuis heeft kenbaar gemaakt dat zij geen opmerkingen op het verslag heeft.

1.3 Aanleiding onderzoek

Op 4 april 2018 heeft het HagaZiekenhuis een melding van een datalek bij de AP gedaan. Het datalek had betrekking op onrechtmatige inzage in een patiëntendossier van een bekende Nederlander. In de melding maakt HagaZiekenhuis kenbaar dat zij in afwachting van het interne onderzoek naar onrechtmatige inzage van dit patiëntendossier beveiligingsmaatregelen zal treffen.

De resultaten van dit interne onderzoek zijn opgenomen in het rapport "Eindrapportage Onderzoek onrechtmatige inzage patiëntdossier" van mei 2018. In dit rapport staat dat het HagaZiekenhuis structureel steekproefsgewijs controleert of bevoegde medewerkers binnen de geldende kaders patiëntendossiers raadplegen. Bij twijfel volgt een onderzoek. Zo volgde ook een onderzoek naar de

(mogelijk) onrechtmatige inzage van het patiëntendossier waar het datalek op ziet, aldus het rapport.[3] In het rapport staat dat in de onderzochte periode 197 medewerkers, waarvan 100 onrechtmatig,[4] inzage hebben gehad in het patiëntendossier. Het HagaZiekenhuis trekt de conclusie dat de oplossing moet leiden tot een structurele verbetering, waarvoor de aanwezige en toekomstige maatregelen die daarin worden genoemd regelmatig getoetst dienen te worden op juiste werking en indien nodig moeten worden bijgesteld.[5]

Naar aanleiding van voormeld rapport heeft de AP in oktober 2018 besloten onder meer nader onderzoek te doen naar de beveiligingsmaatregelen van het HagaZiekenhuis.

2. Wettelijk kader

2.1 Reikwijdte AVG

Ingevolge artikel 2, eerste lid, van de AVG is deze verordening van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Ingevolge artikel 3, eerste lid, is deze verordening van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Unie, ongeacht of de verwerking in de Unie al dan niet plaatsvindt.

Ingevolge artikel 4 wordt voor de toepassing van deze verordening verstaan onder:
1. "Persoonsgegevens": alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); [...].
2. "Verwerking": een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés [...].
7. "Verwerkingsverantwoordelijke": een [...] rechtspersoon die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; [...].
15. "Gegevens over gezondheid": persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.

2.2 Beveiligingsverplichting

2.2.1 AVG

Ingevolge artikel 32, eerste lid, van de AVG treft de verwerkingsverantwoordelijke [...], rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en

[3] Pag. 3 van het rapport.
[4] In de reactie van 4 februari 2019 stelt het HagaZiekenhuis dat dit moet zijn 85.
[5] Pag. 7 van het rapport.

vrijheden van personen, passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen [...].
Ingevolge het tweede lid wordt bij de beoordeling van het passende beveiligingsniveau met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

2.2.2 Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg

Ingevolge artikel 1, aanhef en onder m, van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg wordt in deze wet en de daarop berustende bepalingen verstaan onder:
"Zorginformatiesysteem": elektronisch systeem van een zorgaanbieder voor het verwerken van persoonsgegevens in een dossier, niet zijnde een elektronisch uitwisselingssysteem.

Ingevolge artikel 15j, eerste lid, kunnen bij algemene maatregel van bestuur regels worden gesteld over de functionele, technische en organisatorische maatregelen voor het beheer, de beveiliging en het gebruik van een zorginformatiesysteem of een elektronisch uitwisselingssysteem.

2.2.3 Besluit elektronische gegevensverwerking door zorgaanbieders

Het Besluit elektronische gegevensverwerking door zorgaanbieders is een algemene maatregel van bestuur als bedoeld in artikel 15j, eerste lid, van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg.

Ingevolge artikel 1 wordt in het Besluit elektronische gegevensverwerking door zorgaanbieders verstaan onder:
"NEN 7510": norm voor het organisatorisch en technisch inrichten van de informatiebeveiliging in de zorg;
"NEN 7513": nadere invulling van NEN 7510 betreffende het vastleggen van acties op elektronische patiëntdossiers.
"Zorginformatiesysteem": elektronisch systeem van een zorgaanbieder voor het verwerken van persoonsgegevens in een dossier als bedoeld in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg, niet zijnde een elektronisch uitwisselingssysteem.

Ingevolge artikel 3, tweede lid, draagt een zorgaanbieder overeenkomstig het bepaalde in NEN 7510 [...] zorg voor een veilig en zorgvuldig gebruik van het zorginformatiesysteem [...].

Ingevolge artikel 5, eerste lid, draagt de zorgaanbieder als verantwoordelijke voor een zorginformatiesysteem [...] er zorg voor dat de logging van het systeem voldoet aan het bepaalde in NEN 7513.

2.2.4 NEN 7510 en NEN 7513

NEN 7510 van december 2017 ziet op Medische informatica en Informatiebeveiliging in de zorg en bestaat uit twee delen: deel 1 (7510-1) bevat normatieve voorschriften voor het managementsysteem en deel 2 (7510-2) bevat de beheersmaatregelen. NEN 7513 ziet onder meer op logging. In NEN 7510 en 7513 staat

centraal dat informatie in de zorg vaak vertrouwelijk van aard is. Als zorgorganisatie moeten er dus maatregelen getroffen worden om patiëntgegevens veilig te houden.

Tweefactor authenticatie
In Hoofdstuk 9 (Toegangsbeveiliging), paragraaf 9.4 (Toegangsbeveiliging van systeem en toepassing), onder 9.4.1 (Beperkte toegang tot informatie) van NEN 7510 -2 staat dat gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, de identiteit van gebruikers behoren vast te stellen. Dit behoort te worden gedaan door middel van authenticatie waarbij ten minste twee factoren betrokken worden.

(Controle op) logging
In Hoofdstuk 5 (Informatiebehoeften), paragraaf 5.1 (Algemeen) van NEN 7513 staat dat de logging in het algemeen het mogelijk moet maken dat achteraf onweerlegbaar vast te stellen is welke gebeurtenissen hebben plaatsgevonden op een patiëntendossier. Daartoe moeten alle systemen die gegevens bevatten die deel uitmaken van een patiëntdossier, daarover ten minste bijhouden:
- welke gebeurtenis heeft plaatsgevonden;
- datum en tijdstip van de gebeurtenis;
- welke cliënt het betrof;
- wie de gebruiker was;
- wie de verantwoordelijke gebruiker was namens wie de gebruiker optrad.

In hoofdstuk 12 (Beveiliging bedrijfsvoering), paragraaf 12.4 (Verslaglegging en monitoren), onder 12.4.1 (Gebeurtenissen registreren) van NEN 7510 -2 staat dat logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.

2.3 Bestuurlijke boete en last onder dwangsom

Ingevolge artikel 58, tweede lid, aanhef en onder d en i, in samenhang met artikel 83, vierde lid, aanhef en onder a, van de AVG en artikel 14, derde lid, van de UAVG is de AP onder meer bevoegd om ten aanzien van inbreuken op de AVG een bestuurlijke boete en een last onder dwangsom op te leggen.

2.3.1 AVG
Ingevolge artikel 58, tweede lid, van de AVG heeft elk toezichthoudende autoriteit de bevoegdheid tot het nemen van de volgende corrigerende maatregelen:
d. de verwerkingsverantwoordelijke [...] gelasten, waar passend, op een nader bepaalde manier en binnen een nader bepaalde termijn, verwerkingen in overeenstemming te brengen met de bepalingen van deze verordening;
i. naargelang de omstandigheden van elke zaak, naast of in plaats van de in dit lid bedoelde maatregelen, een administratieve geldboete opleggen op grond van artikel 83.

Ingevolge artikel 83, eerste lid, zorgt elke toezichthoudende autoriteit ervoor dat de administratieve geldboeten die uit hoofde van dit artikel worden opgelegd voor de in de leden 4, 5 en 6 vermelde inbreuken op deze verordening in elke zaak doeltreffend, evenredig en afschrikkend zijn.
Ingevolge het tweede lid worden administratieve geldboeten, naargelang de omstandigheden van het concrete geval, opgelegd naast of in plaats van de in artikel 58, tweede lid, onder a tot en met h en onder j, bedoelde maatregelen.
Uit het vierde lid, aanhef en onder a, volgt dat een inbreuk op de verplichting van de verwerkingsverantwoordelijke van artikel 32 overeenkomstig lid 2 onderworpen is aan een administratieve geldboete tot € 10.000.000 of, voor een onderneming, tot 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is.

2.3.2 Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)

Ingevolge artikel 14, derde lid, van de UAVG kan de AP in geval van overtreding van het bepaalde in artikel 83, vierde lid [...], van de verordening een bestuurlijke boete opleggen van ten hoogste de in deze leden genoemde bedragen.

3. Beoordeling

In paragraaf 3.1 wordt eerst de bevoegdheid van de AP beoordeeld. Vervolgens wordt in paragraaf 3.2 uiteengezet wie voor welke verwerking kan worden aangemerkt als verwerkingsverantwoordelijke. De overtreding van artikel 32, eerste lid, van de AVG, gelezen in samenhang met artikel 3, tweede lid, van het Besluit elektronische gegevensverwerking door zorgaanbieders en het bepaalde onder 9.4.1 en onder 12.4.1 van NEN 7510-2, wordt in paragraaf 3.3 vastgesteld.

3.1 Bevoegdheid AP

Het HagaZiekenhuis heeft een ziekenhuisinformatiesysteem als bedoeld in artikel 1 van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg en artikel 1 van het Besluit elektronische gegevensverwerking door zorgaanbieders. In dit systeem, ook wel genoemd het Elektronisch Patiëntendossier (EPD) of HiX, worden door het HagaZiekenhuis gegevens met betrekking tot patiënten opgenomen. Derhalve is sprake van een verwerking van persoonsgegevens, waaronder persoonsgegevens over gezondheid, als bedoeld in artikel 4 van de AVG.

Ten tijde van voornoemd datalek en de melding door het HagaZiekenhuis aan de AP op 4 april 2018 gold de Wet bescherming persoonsgegevens (Wbp). De Wbp is ingetrokken op 25 mei 2018.[6] Op die dag is de AVG van toepassing geworden[7] en de UAVG in werking getreden.[8]

Naar aanleiding van voornoemd datalek en het daartoe door het HagaZiekenhuis opgestelde rapport "Eindrapportage Onderzoek onrechtmatige inzage patiëntdossier" van mei 2018 heeft de AP in oktober

[6] Artikel 51 van de UAVG.
[7] Artikel 99, tweede lid, van de AVG.
[8] Koninklijk besluit van 16 mei 2018 (Staatsblad 2018, 145).

2018 - ruim na de datum waarop de AVG van toepassing is geworden - een nader onderzoek gestart naar de op dat moment door het HagaZiekenhuis getroffen beveiligingsmaatregelen teneinde te waarborgen dat persoonsgegevens in het digitale patiëntendossier niet worden ingezien door onbevoegde medewerkers. Het onderzoek richtte zich onder meer op de vraag of de door het in Den Haag gevestigde HagaZiekenhuis getroffen beveiligingsmaatregelen met betrekking tot de toegang tot het ziekenhuisinformatiesysteem voldoen aan - het op dat moment vigerende - artikel 32 van de AVG. De AP is ter zake van de in het definitieve rapport geconstateerde overtreding op grond van artikel 58, tweede lid, aanhef en onder d en i, in samenhang met artikel 83, vierde lid, aanhef en onder a, van de AVG en artikel 14, derde lid, van de UAVG bevoegd om een bestuurlijke boete en een last onder dwangsom op te leggen, indien de omstandigheden daartoe aanleiding geven.

3.2 Verwerkingsverantwoordelijke

Het HagaZiekenhuis maakt sinds 12 juli 2013 deel uit van RHG. RHG is een samenwerkingsverband tussen het HagaZiekenhuis, Reinier de Graaf Groep (beide per 12 juli 2013) en het Langeland Ziekenhuis (per 9 juni 2015). In het kader van de vraag of artikel 32, eerste lid, van de AVG wordt nageleefd, is van belang om te bepalen wie is of zijn aan te merken als (gezamenlijke) verwerkingsverantwoordelijke(n) als bedoeld in artikel 4, onder 7, van de AVG. Daarbij is bepalend wie het doel van en de middelen voor de verwerking van persoonsgegevens - in dit geval de verwerking van patiëntgegevens in het ziekenhuisinformatiesysteem van het HagaZiekenhuis - vaststelt. Om deze vraag te beantwoorden hecht de AP waarde aan het bepaalde in het rapport "Informatiebeveiligingsbeleid Reinier Haga Groep" van 25 december 2015 (Informatiebeveiligingsbeleid), het rapport Autorisatie Digitale Patiënten Dossiers van mei 2018 (Autorisatiebeleid), de Privacyverklaring van het HagaZiekenhuis[9] en de verklaring van [VERTROUWELIJK] zoals opgenomen in Verslag van gesprekken OTP HagaZiekenhuis.

3.2.1 Informatiebeveiligingsbeleid

Zoals tevens door het HagaZiekenhuis ter zienswijzezitting is bevestigd, is het algemene deel van het door RHG vastgestelde Informatiebeveiligingsbeleid van toepassing op alle gegevensverwerkingen in alle vestigingsadressen van RHG, waaronder het HagaZiekenhuis.[10] Bij de toepassing van informatiebeveiliging binnen RHG worden de normen NEN 7510 en NEN 7513 als uitgangspunt gehanteerd.[11] Deze normen worden in het algemene deel van het Informatiebeveiligingsbeleid niet verder uitgewerkt. De Raad van Bestuur van RHG is bestuurlijk verantwoordelijk voor de uitvoering van het beleid en de maatregelen op gebied van informatiebeveiliging.[12]

De lokale invulling van het algemene deel - hetgeen per organisatie binnen RHG kan verschillen - is opgenomen in de bijlagen bij het Informatiebeveiligingsbeleid. Bijlage 2 ziet op de lokale invulling door het HagaZiekenhuis. Het HagaZiekenhuis heeft een eigen Information Security Officer (ISO), die het dagelijks

[9] https://www.hagaziekenhuis.nl/over-hagaziekenhuis/goed-om-te-weten/patiëntenrechten/privacyverklaring.aspx.
[10] Pag. 4 Informatiebeveiligingsbeleid. In aanvulling hierop heeft het HagaZiekenhuis desgevraagd bevestigd dat het algemene deel van dit beleid ook van toepassing is op stichting Stichting Langeland Ziekenhuis.
[11] Pag. 9 Informatiebeveiligingsbeleid.
[12] Pag. 6 Informatiebeveiligingsbeleid.

aanspreekpunt is voor alle aangelegenheden voor informatiebeveiliging binnen dat ziekenhuis en de lokale coördinatie van activiteiten aangaande informatiebeveiliging uitvoert.[13] Alle onderdelen van RHG moeten adequate maatregelen hebben getroffen om de continuïteit van de operationele werkzaamheden te borgen. Het beheren van - onder meer - een noodknopprocedure, vormt hiervan een onderdeel.[14] De normen NEN 7510 en NEN 7513 worden in Bijlage 2 (Lokale invulling HagaZiekenhuis) niet verder uitgewerkt.

3.2.2 Autorisatiebeleid

Het Autorisatiebeleid is door het HagaZiekenhuis opgesteld en bevat beleid voor de inrichting en systemen in verband met autorisatie voor toegang tot het EPD binnen het HagaZiekenhuis, alsmede de controle daarop.[15] In dit beleid staat dat in ziekenhuizen het doel en de middelen voor de verwerking van persoonsgegevens worden bepaald door de directie van het HagaZiekenhuis.[16] De directie neemt passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.[17]

3.2.3 Privacyverklaring

In de Privacyverklaring van het HagaZiekenhuis staat dat deze van toepassing is op de verwerking van persoonsgegevens door het HagaZiekenhuis. Het HagaZiekenhuis heeft ter zienswijzezitting toegelicht dat het Privacyreglement van RHG van 15 juni 2017 als basis dient voor de Privacyverklaring. De AP merkt op dat het Privacyreglement uitsluitend bepalingen op hoofdlijnen bevat die zien op de verwerking van persoonsgegevens. De Privacyverklaring bevat een nadere invulling van het Privacyreglement, op grond waarvan gegevensverwerking door het HagaZiekenhuis voor - onder meer - de volgende daarin opgenomen doeleinden kan worden verwerkt:
- het verlenen, berekenen van de kosten en declareren van zorg;
- het verrichten van wetenschappelijk onderzoek;
- het opleiden en onderwijzen van zorgpersoneel;
- administratie en interne beheersactiviteiten;
- kwaliteitsbewaking en -bevordering van de zorgverlening.

Verder staat er in de Privacyverklaring dat het HagaZiekenhuis ook samenwerkt met andere zorginstellingen. Het HagaZiekenhuis vraagt toestemming van de patiënt voordat zij de betreffende gegevens uitwisselen, tenzij de belangen van de patiënt of een derde in gevaar zijn.

3.2.4 Verklaring HagaZiekenhuis

Op 31 oktober 2018 heeft [VERTROUWELIJK] van het HagaZiekenhuis tijdens het OTP verklaard dat RHG een bestuurlijke fusie en geen juridische fusie betreft. Zo zijn de ziekenhuizen systeemtechnisch gescheiden, is de uitwerking van het Autorisatiebeleid per ziekenhuis anders en wordt het algemeen Informatiebeveiligingsbeleid lokaal per ziekenhuis ingevuld. Elk ziekenhuis heeft ook een eigen

[13] Pag. 6 van het Informatiebeveiligingsbeleid.
[14] Pag. 11 van het Informatiebeveiligingsbeleid.
[15] Pag. 3 Autorisatiebeleid.
[16] Pag. 2 Autorisatiebeleid.
[17] Pag. 3 Autorisatiebeleid.

Autorisatiecommissie.[18]

3.2.5 Beoordeling AP

De AP is van oordeel dat het HagaZiekenhuis doelen en middelen van de gegevensverwerking in het ziekenhuisinformatiesysteem van het HagaZiekenhuis - dat gescheiden is van de ziekenhuisinformatiesystemen van de andere ziekenhuizen van RHG - bepaalt. Zo bepaalt zij zelfstandig de lokale invulling van het algemene Informatiebeveiligingsbeleid en heeft zij een eigen Autorisatiebeleid, aan de hand waarvan zij bepaalt wie geautoriseerde toegang mag hebben tot welke patiëntgegevens. Ook heeft het HagaZiekenhuis een eigen Privacyverklaring, waarin zij de doeleinden van gegevensverwerking door het HagaZiekenhuis bepaalt.

Voor de vraag of het HagaZiekenhuis alleen of samen met RHG beslissingen neemt met betrekking tot de vaststelling van doelen en middelen van de gegevensverwerking in het ziekenhuisinformatiesysteem van het HagaZiekenhuis, is van belang dat RHG uitsluitend een algemeen Informatiebeveiligingsbeleid en een algemeen Privacyreglement heeft vastgesteld. Dit vastgestelde algemene beleid ziet niet op detailniveau toe op hoe de ziekenhuizen binnen RHG het ziekenhuisinformatiesysteem inrichten. Het Informatiebeveiligingsbeleid ziet uitsluitend erop dat daarbij de normen NEN 7510 en NEN 7513 in acht dienen te worden genomen. Dit volgt eveneens uit artikel 32, eerste lid, van de AVG, gelezen in samenhang met artikel 3, tweede lid, en artikel 5, tweede lid, van het Besluit elektronische gegevensverwerking door zorgaanbieders. Het Privacyreglement bevat verder uitsluitend een herhaling van de normen uit de destijds geldende Wbp, zonder daarbij deze normen concreet in te vullen. Verder valt het samenwerkingsverband buiten het bereik van het Autorisatiebeleid - dat ziet op de autorisatie voor toegang tot het EPD van het HagaZiekenhuis - en de Privacyverklaring van het HagaZiekenhuis, waarin onder meer de doelen van de gegevensverwerking voor het HagaZiekenhuis zijn opgenomen.

Mede gelet op de verklaring van [VERTROUWELIJK] van het HagaZiekenhuis is de AP met inachtneming van het voorgaande van oordeel dat het HagaZiekenhuis zelfstandig de formeel-juridische bevoegdheid heeft om doelen en middelen van de gegevensverwerking in het ziekenhuisinformatiesysteem van het HagaZiekenhuis vast te stellen.

3.2.6 Conclusie

Nu het HagaZiekenhuis zich ten aanzien van het ziekenhuisinformatiesysteem naar het oordeel van de AP autonoom opstelt, wordt het HagaZiekenhuis - en niet daarnaast ook RHG - met betrekking tot gegevensverwerkingen in dat ziekenhuisinformatiesysteem als verwerkingsverantwoordelijke als bedoeld in artikel 4, aanhef en onder 7, van de AVG aangemerkt.

3.3 Overtreding inzake gegevensbeveiliging

3.3.1 Inleiding

Om de veiligheid te waarborgen en te voorkomen dat de verwerking van persoonsgegevens inbreuk maakt

[18] Pag. 2 van het Verslag van gesprekken OTP HagaZiekenhuis.

op de AVG, dient de verwerkingsverantwoordelijke op grond van artikel 32 van de AVG de aan de verwerking inherente risico's te beoordelen en maatregelen te treffen om risico's te beperken. Die maatregelen dienen een passend niveau van beveiliging te waarborgen, rekening houdend met de stand van de techniek en de uitvoeringskosten afgezet tegen de risico's en de aard van de te beschermen persoonsgegevens.[19] Gezondheidsgegevens behoren vanwege de gevoeligheid tot een bijzondere categorie van persoonsgegevens. Om deze reden gelden voor de bescherming van die gegevens zeer hoge eisen.

Met passende beveiligingsmaatregelen wordt bijgedragen aan het behoud van vertrouwen van patiënten in het desbetreffende ziekenhuis bij de omgang met persoonsgegevens. Om te bepalen of beveiligingsmaatregelen passend zijn, dient in het voorliggende geval te worden aangesloten bij algemeen geaccepteerde beveiligingsstandaarden binnen de praktijk van de informatiebeveiliging in de zorg, NEN-7510 en NEN 7513. Uit deze beveiligingsstandaarden vloeit voort dat ten aanzien van authenticatie bij de toegang tot ziekenhuisinformatiesystemen die specifiek zijn gericht op het verwerken van gevoelige informatie, de verantwoordelijke tenminste gebruik dient te maken van tweefactor authenticatie, teneinde de identiteit van gebruikers vast te stellen. Verder dienen logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, te worden gemaakt, bewaard en regelmatig te worden beoordeeld. Het voorgaande volgt uit NEN 7510 -2, waarin beveiligingsnormen zijn opgenomen die zien op een nadere invulling van artikel 32 van de AVG wat betreft de informatiebeveiliging in de zorg, waarnaar het Autorisatiebeleid van het HagaZiekenhuis eveneens verwijst.

3.3.2 Tweefactor authenticatie

In paragraaf 9.4.1 van NEN 7510 -2 staat dat gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, de identiteit van gebruikers behoren vast te stellen. Dit behoort te worden gedaan door middel van authenticatie waarbij ten minste twee factoren betrokken worden. Dit betekent dat de identiteit van de gebruiker om toegang te krijgen tot het gezondheidsinformatiesysteem bijvoorbeeld wordt vastgesteld op basis van kennis (code of een wachtwoord) en bezit (personeelspas).

Regeling Personeelspas en Gebruikershandleiding Virtuele Werkplek

In de Regeling Personeelspas van het HagaZiekenhuis[20] staat dat alle medewerkers van het HagaZiekenhuis een personeelspas hebben, waarmee kan worden ingelogd op de computers. De bevoegdheden van deze eigen identiteitspas hangen samen met de functie en werkplek van de medewerker. Met deze pas kan worden voorkomen dat andere gebruikers vertrouwelijke documenten kunnen inzien. Het inloggen kan ook zonder pas, maar met gebruikmaking van gebruikersnaam en wachtwoord. De pas is slechts ter vergemakkelijking, aldus de Regeling.

In de Gebruikershandleiding Virtuele Werkplek[21] wordt bevestigd dat de werkstations met een paslezer geschikt zijn voor het virtueel werken. Medewerkers kunnen handmatig, maar na registratie ook met de

[19] Overweging 83 van de AVG.
[20] Revisiedatum 13 juni 2017.
[21] Van 14 augustus 2018.

personeelspas aanmelden.[22]

Verklaring HagaZiekenhuis
Tijdens het OTP op 31 oktober 2018 heeft het HagaZiekenhuis bevestigd dat er op twee manieren kan worden ingelogd op de computers en het ziekenhuisinformatiesysteem. Eén van de mogelijkheden is met gebruikmaking van de personeelspas, die voor de paslezer wordt gehouden, waarna kan worden ingelogd op de Virtual Desktop Infrastructure (VDI) met gebruikersnaam, wachtwoord en een 4 cijferige vaste pincode. Aan dit persoonlijke netwerkaccount hangt een persoonlijk HiX account. Dit betekent dat als een medewerker eenmaal is ingelogd op de VDI, deze medewerker ook toegang heeft tot het ziekenhuisinformatiesysteem. Daarna kan de gebruiker gedurende vier uur - de zogenoemde 'grace period' - op een willekeurig werkstation met de pas af- en aanmelden zonder invoer van gebruikersnaam, wachtwoord en/of pincode. De andere mogelijkheid is zonder gebruikmaking van de personeelspas, waarbij handmatig kan worden ingelogd op de VDI met gebruikersnaam en wachtwoord. Eenmaal ingelogd heeft de medewerker - net als bij het inloggen met de pas - ook toegang tot het ziekenhuisinformatiesysteem.[23]

Zienswijze
In de zienswijze van het HagaZiekenhuis staat dat in de huidige situatie toegang tot het ziekenhuisinformatiesysteem kan worden verkregen zowel via tweefactor - als via eenfactor authenticatie. Tijdens de zienswijzezitting is toegelicht dat het HagaZiekenhuis in 2012 is aangevangen met de virtuele werkplekken, tevens met de mogelijkheid om handmatig in te loggen. Zij heeft zich ten doel gesteld om per 1 oktober 2019 ziekenhuisbreed permanente tweefactor authenticatie te hebben geïmplementeerd, waarbij de mogelijkheid om in te loggen via eenfactor authenticatie verdwijnt. Verder zal het HagaZiekenhuis de zogenoemde 'grace period' afschaffen, zodat bij toegang via tweefactor authenticatie telkens om een pincode zal worden gevraagd.

Beoordeling AP
Nu de sterkte van de gebruikersauthenticatie passend behoort te zijn voor de classificatie van de informatie waartoe toegang wordt verleend, en in het ziekenhuisinformatiesysteem (met name) gegevens over gezondheid worden verwerkt, is tweefactor authenticatie vereist. De AP stelt vast - en evenmin in geschil is - dat authenticatie in het HagaZiekenhuis tot het ziekenhuisinformatiesysteem in ieder geval sinds januari 2018 heeft plaatsgevonden en nog steeds plaatsvindt met gebruikmaking van de unieke personeelspas. In de andere situatie, inloggen zonder personeelspas, vindt authenticatie plaats op basis van een gebruikersnaam en wachtwoord, waarna het ziekenhuisinformatiesysteem geraadpleegd kan worden. De identiteit van de gebruiker om toegang te krijgen tot dit systeem kan in dit geval aldus plaatsvinden uitsluitend op basis van kennis (code of een wachtwoord), zonder bezit (personeelspas). Derhalve is een enkelvoudige methode voor raadpleging van het ziekenhuisinformatiesysteem door de gebruikers niet uit te sluiten en ontbreekt een noodzakelijk benodigde tweede factor die bijdraagt aan een passend beveiligingsniveau. Daarmee wordt niet voldaan aan het vereiste van tweefactor authenticatie

[22] Pag. 2 Gebruikershandleiding Virtuele Werkplek.
[23] Pag. 7 Verklaring van gesprekken OTP HagaZiekenhuis en tevens bevestigd ter zienswijzezitting.

ingevolge artikel 32 van de AVG, gelezen in samenhang met artikel 3, tweede lid, Besluit elektronische gegevensverwerking door zorgaanbieders en het bepaalde onder 9.4.1 van NEN 7510 -2.

3.3.3 Regelmatig beoordelen van logbestanden

Zorginstellingen moeten structureel bijhouden wie wanneer welk patiëntendossier heeft geraadpleegd (logging) en dit moet regelmatig worden gecontroleerd. Op deze manier kan de instelling onbevoegde toegang signaleren en maatregelen nemen. Dit is gebaseerd op paragraaf 12.4.1 van NEN 7510 -2, waarin staat dat logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.

Onder verwijzing naar het rapport "Toegang tot digitale patiëntendossiers binnen zorginstellingen" van juni 2013 is het uitgangspunt van de AP[24] dat controle van de logging systematisch en consequent moet plaatsvinden, waarbij een steekproefsgewijze controle en/of controle op basis van klachten niet voldoende is. Daarbij is van belang dat bij een willekeurig steekproefsgewijs controleren geen sprake is van een systematiek gericht op onrechtmatig gebruik en risico's.

Autorisatiebeleid

In het Autorisatiebeleid van het HagaZiekenhuis staat dat beveiliging en logging overeenkomstig de uitgangspunten zoals gesteld in de NEN 7510 en NEN 7513 dienen plaats te vinden. In het Autorisatiebeleid is als uitgangspunt opgenomen dat de logbestanden periodiek worden gecontroleerd op indicaties van onrechtmatige toegang of onrechtmatig gebruik van persoonsgegevens en waar nodig actie wordt ondernomen door de verantwoordelijke. Het Autorisatiebeleid maakt onderscheid in de controle van (1) reguliere patiëntendossiers, (2) patiëntendossiers die behoren tot specialismen en (3) patiëntendossiers waartoe toegang is verkregen via de zogenoemde noodknopprocedure, ook wel aangeduid als 'breaking the glass' - procedure, hieronder nader beschreven.[25]

De FG dient op grond van het Autorisatiebeleid voor (1) de reguliere patiëntendossiers eens per twee maanden een audit uit te voeren op toegang tot het systeem conform de vastgestelde autorisatieprocedure. Het HagaZiekenhuis heeft bij de zienswijzezitting toegelicht dat hieronder moet worden begrepen een controle van één patiëntendossier per twee maanden. Het HagaZiekenhuis heeft verder toegelicht dat (2) indien een geselecteerd dossier hoort tot behandeling in de specialismen psychiatrie, psychologie, VIP, eigen personeel en in relatie tot geslachtsziektes, de logging van dat dossier volledig dient te worden gecontroleerd. Dit houdt in dat de logging van dit dossier voor een langere periode wordt gecontroleerd. Medewerkers van het HagaZiekenhuis kunnen tevens gebruik maken van (3) een noodknopprocedure, waarmee zij toegang verkrijgen tot gegevens van een patiënt, waartoe deze medewerker niet geautoriseerd is. De procedure laat bij het zoeken van dergelijke patiëntgegevens en bij het daadwerkelijk in willen kijken van deze gegevens een melding op het scherm zien, waarin medewerkers erop worden gewezen dat zij niet bevoegd zijn om toegang te krijgen tot deze specifieke patiëntgegevens. Aan de medewerkers wordt

[24] Weliswaar onder de werking van de Wbp, maar de strekking van artikel 32 van de AVG is ten opzichte van artikel 13 van de destijds geldende Wbp niet gewijzigd.
[25] Pag. 3 van het Autorisatiebeleid.

gevraagd een reden op te geven waarom toegang toch noodzakelijk is. Met behulp van die procedure kunnen medewerkers dan alsnog ruimer toegang verkrijgen tot gegevens van patiënten. In het Autorisatiebeleid staat dat een mislukte toegangspoging alsmede gerealiseerde toegang tot een digitaal dossier van een patiënt, die gerealiseerd worden via de noodknopprocedure, via de logging regulier dienen te worden gecontroleerd op rechtmatigheid.

Verklaring HagaZiekenhuis
[VERTROUWELIJK] heeft tijdens het OTP verklaard dat elke handeling in het EPD wordt gelogd. De controles op de logging worden uitgevoerd door de ISO en de FG. De eerste controle in 2018 betrof het patiëntendossier van de bekende Nederlander, gelet op de grote hoeveelheid inzagen in dit specifieke dossier.[26] Op verzoek van patiënten en medewerkers heeft het HagaZiekenhuis in 2018 nog meer controles uitgevoerd, waaruit geen misstanden naar voren zijn gekomen. [VERTROUWELIJK] heeft verder verklaard dat het HagaZiekenhuis voornemens is in 2019 zes aselecte steekproeven per jaar in het kader van controle van de logging conform het Autorisatiebeleid uit te voeren, waarbij zes verschillende patiënten van verschillende afdelingen zullen worden gecontroleerd. In verband met de drukte wegens voormeld datalek en de vervolgacties daarop, was het HagaZiekenhuis ten tijde van de verklaring van 31 oktober 2018 (nog) niet hieraan toegekomen.

Zienswijze
Het HagaZiekenhuis beoogt uiterlijk 1 oktober 2019 te voldoen aan paragraaf 12.4.1 van NEN 7510 -2 in de vorm van het voeren van controle op logging op de volgende drie manieren: (1) op basis van steekproeven die zes patiëntendossiers per jaar beslaan, (2) op basis van klachten en verzoeken van de patiënt en (3) door middel van een systematische analyse van het gebruik van de noodknopprocedure. De steekproef (1) is beperkt tot zes dossiers per jaar omdat het uitvoeren van een dergelijke controle een zeer arbeidsintensief proces is, aldus het HagaZiekenhuis. Na het genereren van de logging moet handmatig per loggingsregel worden bepaald of degene die inlogt deel uitmaakt van het behandelteam van de betreffende patiënt. Ter zienswijzezitting heeft het HagaZiekenhuis desgevraagd een ruwe inschatting gemaakt van de omvang van het controletraject, dat bestaat uit vijf stappen. De eerste drie stappen kunnen worden uitgevoerd door één medewerker en zien op het genereren van de logging, het aanvullen en controleren en het vaststellen van het behandelteam. In de laatste twee stappen vindt verder onderzoek plaats, uitgevoerd door meerdere medewerkers. De uitvoering van de eerste drie stappen duren in totaal - en gemiddeld - ongeveer acht uur, hetgeen ongeveer een derde tot de helft van een volledig controletraject beslaat, aldus het HagaZiekenhuis. Ten aanzien van de controle op logging maakt zij verder kenbaar dat (2) patiënten ook recht op inzage op de logging kunnen inroepen en het HagaZiekenhuis in die gevallen ook controle op logging uitvoert. De systematische analyse (3) omvat een wekelijkse controle van de logging van alle patiëntendossiers die zijn geraadpleegd via de noodknopprocedure. De door haar opgestelde planning gericht op 1 oktober 2019 gaat uit van een handmatige controle. De mogelijkheden van inzet van [VERTROUWELIJK] - als technisch hulpmiddel bij het uitvoeren van de controle op de logging - worden door het HagaZiekenhuis nog onderzocht.

Ter zienswijzezitting heeft het HagaZiekenhuis bevestigd dat zij in de periode van januari 2018 tot en met

[26] Zie ook de reactie van het HagaZiekenhuis van 4 februari 2019.

oktober 2018 proactief één controle op logging met betrekking tot het dossier van de bekende Nederlander en zes controles op logging met betrekking tot zes dossiers op verzoeken van patiënten en medewerkers heeft uitgevoerd. Na oktober 2018 hebben nog diverse controles op verzoek van patiënten en/of medewerkers plaatsgevonden. In januari 2019 is het HagaZiekenhuis begonnen met de eerste steekproef van de voorgenomen zes steekproeven per jaar. Het tweede onderzoek staat voor april/mei 2019 op de planning, aldus het HagaZiekenhuis.

Beoordeling AP
De AP stelt vast dat het HagaZiekenhuis in 2018 de controle - uitgezonderd één proactieve steekproef - uitsluitend naar aanleiding van enkele klachten en verzoeken heeft uitgevoerd. De in 2019 gedane proactieve controle (betrekking op maximaal twee patiëntdossiers) omvat niet tevens een afzonderlijke controle van de logging van patiëntendossiers die zijn geraadpleegd via de noodknopprocedure. Het HagaZiekenhuis heeft daarmee in ieder geval gedurende voornoemde periode (januari 2018 tot heden) niet conform haar eigen Autorisatiebeleid gehandeld. Afgezien daarvan, is het doen van slechts één of enkele proactieve steekproef/steekproeven per jaar ruimschoots en evident onvoldoende om te kunnen spreken van een passend beveiligingsniveau dat ziet op het signaleren van onbevoegde toegang tot patiëntgegevens en het treffen van maatregelen naar aanleiding van onbevoegde toegang. Daarbij acht de AP van belang de schaal van de verwerking van gezondheidsgegevens door het ziekenhuis[27] en het ontbreken van een regelmatige controle op gebruikmaking van de noodknopprocedure, als gevolg waarvan medewerkers toegang kunnen verkrijgen tot meer gegevens dan waartoe zij in eerste instantie bevoegd zijn. Gelet hierop is geen sprake van passende maatregelen ten aanzien van controle van de logging zoals vereist is ingevolge artikel 32, eerste lid, van de AVG, gelezen in samenhang met artikel 3, tweede lid, Besluit elektronische gegevensverwerking door zorgaanbieders en het bepaalde onder 12.4.1 van NEN 7510-2.

Daarnaast beantwoordt de AP in het kader van de op te leggen last onder dwangsom tevens de vraag of het Autorisatiebeleid voorziet in een systematische, consequente controle van de gegevens van het loggen. De AP stelt mede aan de hand van de toelichting van het HagaZiekenhuis vast dat het Autorisatiebeleid voorziet in een controle op de logging van zes (al dan niet reguliere) patiëntendossiers en een reguliere controle van patiëntendossiers ten aanzien waarvan de toegang is verkregen met gebruikmaking van de noodknopprocedure. Wat onder reguliere controle van laatstgenoemde dossiers moet worden verstaan, wordt in het Autorisatiebeleid niet verder uitgewerkt. In de zienswijze van het HagaZiekenhuis van 18 april 2019 staat dat zij beoogt om uiterlijk op 1 oktober 2019 wekelijks alle patiëntendossiers te onderzoeken die via de noodknopprocedure zijn geraadpleegd. Het HagaZiekenhuis stelt zich met de implementatie van de voorgenomen maatregelen, naast de reactieve controle naar aanleiding van een klacht of een verzoek, op het standpunt dat de logbestanden regelmatig worden gecontroleerd als bedoeld in de NEN 7510-2. Een dergelijke wekelijkse controle voldoet naar het oordeel van de AP zonder meer aan het vereiste van een systematische, consequente controle van de gegevens van het loggen. Dit laat evenwel onverlet dat het HagaZiekenhuis eveneens het risico op misbruik binnen het autorisatieprofiel ten aanzien

[27] In dit kader verwijst de AP naar de door het HagaZiekenhuis ter zienswijzezitting overgelegde cijfers uit het Jaarverslag. In 2017 had het HagaZiekenhuis (afgerond) 28.500 opnamen, 158.000 eerste polikliniekbezoeken, 52.000 eerste hulp consulten en 143.000 verpleegdagen.

van de overige - niet via de noodknopprocedure geraadpleegde - dossiers in voldoende mate dient te beheersen. Aan de hand van logbestanden kan worden achterhaald wie toegang had tot welke gezondheidsgegevens. Op een omvang van - in 2017 - (afgerond) 28.500 opnamen, 158.000 eerste polikliniekbezoeken, 52.000 eerste hulp consulten en 143.000 verpleegdagen, biedt een controle van jaarlijks zes patiëntendossiers onvoldoende inspanning om gevallen van onrechtmatige verwerkingen die plaatsvinden binnen de autorisatie in voldoende mate te kunnen detecteren. Naar het oordeel van de AP leidt dit aldus niet tot het vereiste passende beveiligingsniveau in de gevallen dat het dossier binnen de autorisatie is geraadpleegd.

De huidige stand van de techniek is maatgevend voor hetgeen als passende maatregelen in de zin van artikel 32, eerste lid, van de AVG kan worden beschouwd. Het HagaZiekenhuis heeft niet aannemelijk gemaakt dat er - eventueel naast [VERTROUWELIJK] - geen andere technische ondersteuningsmogelijkheden beschikbaar zijn. De stappen gezet door het HagaZiekenhuis om te komen tot een update in dat kader, zijn dan ook aangewezen. Voor zover het HagaZiekenhuis geen of beperkte technische ondersteuning heeft om de controle van logging uit te voeren of te ondersteunen, zoals zij heeft aangevoerd in de zienswijze, dient zij de controle van de logging organisatorisch in te regelen. Het HagaZiekenhuis heeft daartoe het voorstel gedaan de logging van alle dossiers die zijn geraadpleegd via de noodknopprocedure handmatig te controleren. Gelet daarop valt niet in te zien dat een handmatige controle van de logging van meer dan zes - niet via de noodknopprocedure geraadpleegde - dossiers per jaar, niet van haar kan worden gevergd. Dat het HagaZiekenhuis, zoals zij ter zienswijzezitting heeft toegelicht, ook preventieve maatregelen treft met het oog op voorkoming van onrechtmatige toegang tot patiëntgegevens, die onder meer zien op bewustwording van de medewerkers over het zorgvuldig omgaan met patiëntgegevens, neemt de verplichting tot het treffen van voornoemde passende technische en organisatorische maatregelen in de zin van artikel 32, eerste lid, van de AVG niet weg.

In aanmerking genomen dat het Autorisatiebeleid onder meer ziet op een controle van één steekproef van één dossier per twee maanden, voorziet dat beleid naar het oordeel van de AP in zoverre niet in een systematische, consequente controle van de logging.

3.3.4 Conclusie

Gelet op het voorgaande is de AP van oordeel dat het HagaZiekenhuis artikel 32, eerste lid, van de AVG, gelezen in samenhang met artikel 3, tweede lid, van het Besluit elektronische gegevensverwerking door zorgaanbieders en het bepaalde onder 9.4.1 en onder 12.4.1 van NEN 7510-2, heeft overtreden, nu in de periode van januari 2018 tot op heden niet is voldaan aan het vereiste van tweefactor authenticatie en het regelmatig beoordelen van logbestanden. De overtreding duurt thans voort.

4. Boete

4.1 Inleiding

De door het HagaZiekenhuis getroffen beveiligingsmaatregelen zien niet op een (juiste) implementatie van het hanteren van tweefactor authenticatie en het regelmatig controleren van de logbestanden. Van het

HagaZiekenhuis mag evenwel worden verwacht dat zij zich van de voor haar geldende normen vergewist. Het niet hanteren van tweefactor authenticatie in geval van toegang tot patiëntgegevens - waarin paragraaf 9.4.1 van NEN 7510-2 geen ruimte laat - en het uitsluitend in de praktijk proactief controleren van de logging van één of enkele patiëntendossier(s) gedurende een periode van meer dan een jaar, is naar het oordeel van de AP - en anders dan het HagaZiekenhuis aanvoert - evident en op structurele wijze in strijd met artikel 32, eerste lid, van de AVG, gelezen in samenhang met het bepaalde onder 9.4.1 en onder 12.4.1 van NEN 7510-2. Dat het HagaZiekenhuis ter zienswijzezitting heeft aangevoerd dat de norm in 12.4.1 van NEN 7510-2 een open norm behelst, doet daar - wat daar ook van zij - niet aan af, nu het HagaZiekenhuis in de praktijk tevens is afgeweken van haar eigen Autorisatiebeleid. Dit terwijl het Autorisatiebeleid volgens haar met de uitleg die zij hieraan geeft in de zienswijze voldoet aan de norm in 12.4.1 van NEN 7510-2. De AP ziet in het voorliggende geval aanleiding om gebruik te maken van haar bevoegdheid om een boete op grond van artikel 58, tweede lid, aanhef en onder i en artikel 83, vierde lid, van de AVG, gelezen in samenhang met artikel 14, derde lid, van de UAVG, aan het HagaZiekenhuis op te leggen.

4.2 Boetebeleidsregels Autoriteit Persoonsgegevens 2019 (Boetebeleidsregels 2019)

Ingevolge artikel 58, tweede lid, aanhef en onder i en artikel 83, vierde lid, van de AVG, gelezen in samenhang met artikel 14, derde lid, van de UAVG, is de AP bevoegd aan het HagaZiekenhuis in geval van een overtreding van artikel 32, eerste lid, van de AVG een bestuurlijke boete op te leggen tot € 10.000.000 of tot 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is.

De AP heeft Boetebeleidsregels 2019 vastgesteld inzake de invulling van voornoemde bevoegdheid tot het opleggen van een bestuurlijke boete, waaronder het bepalen van de hoogte daarvan.[28]

Ingevolge artikel 2, onder 2.1, van de Boetebeleidsregels 2019 zijn de bepalingen ter zake van overtreding waarvan de AP een bestuurlijke boete kan opleggen van ten hoogste het bedrag van € 10.000.000 of, voor een onderneming, tot 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is, in bijlage 1 ingedeeld in categorie I, categorie II of categorie III.

In Bijlage I is artikel 32 van de AVG ingedeeld in categorie II.

Ingevolge artikel 2, onder 2.3, stelt de AP de basisboete voor overtredingen waarvoor een wettelijk boetemaximum geldt van € 10.000.000 of, voor een onderneming, tot 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is, […] vast binnen de volgende boetebandbreedte:
Categorie II: Boetebandbreedte tussen € 120.000 en € 500.000 en een basisboete van € 310.000. […].

Ingevolge artikel 6 bepaalt de AP de hoogte van de boete door het bedrag van de basisboete naar boven (tot ten hoogste het maximum van de bandbreedte van de aan een overtreding gekoppelde boetecategorie) of naar beneden (tot ten laagste het minimum van die bandbreedte) bij te stellen. De basisboete wordt

[28] Stcrt. 2019, 14586, 14 maart 2019.

verhoogd of verlaagd afhankelijk van de mate waarin de factoren die zijn genoemd in artikel 7 daartoe aanleiding geven.

Ingevolge artikel 7 houdt de AP onverminderd de artikelen 3:4 en 5:46 van de Algemene wet bestuursrecht (Awb) rekening met de factoren die zijn ontleend aan artikel 83, tweede lid, van de AVG, in de Beleidsregels genoemd onder a tot en met k:
a. de aard, de ernst en de duur van de inbreuk, rekening houdend met de aard, de omvang of het doel van de verwerking in kwestie alsmede het aantal getroffen betrokkenen en de omvang van de door hen geleden schade;
b. de opzettelijke of nalatige aard van de inbreuk;
c. de door de verwerkingsverantwoordelijke [...] genomen maatregelen om de door betrokkenen geleden schade te beperken;
d. de mate waarin de verwerkingsverantwoordelijke [...] verantwoordelijk is gezien de technische en organisatorische maatregelen die hij heeft uitgevoerd overeenkomstig de artikelen 25 en 32 van de AVG;
e. eerdere relevante inbreuken door de verwerkingsverantwoordelijke [...];
f. de mate waarin er met de toezichthoudende autoriteit is samengewerkt om de inbreuk te verhelpen en de mogelijke negatieve gevolgen daarvan te beperken;
g. de categorieën van persoonsgegevens waarop de inbreuk betrekking heeft;
h. de wijze waarop de toezichthoudende autoriteit kennis heeft gekregen van de inbreuk, met name of, en zo ja in hoeverre, de verwerkingsverantwoordelijke [...] de inbreuk heeft gemeld;
i. de naleving van de in artikel 58, tweede lid, van de AVG genoemde maatregelen, voor zover die eerder ten aanzien van de verwerkingsverantwoordelijke [...] in kwestie met betrekking tot dezelfde aangelegenheid zijn genomen;
j. het aansluiten bij goedgekeurde gedragscodes overeenkomstig artikel 40 van de AVG of van goedgekeurde certificeringsmechanismen overeenkomstig artikel 42 van de AVG; en
k. elke andere op de omstandigheden van de zaak toepasselijke verzwarende of verzachtende factor, zoals gemaakte financiële winsten, of vermeden verliezen, die al dan niet rechtstreeks uit de inbreuk voortvloeien.

Ingevolge artikel 9 houdt de AP bij het vaststellen van de boete zo nodig rekening met de financiële omstandigheden waarin de overtreder verkeert. In geval van verminderde of onvoldoende draagkracht van de overtreder kan de AP de op te leggen boete verder gaand matigen, indien, na toepassing van artikel 8.1 van de beleidsregels, vaststelling van een boete binnen de boetebandbreedte van de naast lagere categorie naar haar oordeel desalniettemin zou leiden tot een onevenredig hoge boete.

4.3 Systematiek

Ter zake van overtredingen waarvan de AP een bestuurlijke boete kan opleggen van ten hoogste het bedrag van € 10.000.000 of tot 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is, heeft de AP in de Boetebeleidsregels 2019 de overtredingen ingedeeld in drie categorieën, waaraan in zwaarte oplopende bestuurlijke geldboetes zijn verbonden. De boetecategorieën zijn

gerangschikt naar zwaarte van de overtreding van de genoemde artikelen, waarbij categorie I de minst zware overtredingen bevat en categorie II of III de zwaarste overtredingen.

Overtreding van artikel 32, eerste lid, van de AVG is ingedeeld in categorie II, waarvoor een boetebandbreedte tussen € 120.000 en € 500.000 en een basisboete van € 310.000 is vastgesteld. De AP hanteert de basisboete als neutraal uitgangspunt. De hoogte van de boete stemt de AP ingevolge artikel 6 van de Boetebeleidsregels 2019 vervolgens af op de factoren die zijn genoemd in artikel 7 van de Boetebeleidsregels 2019, door het bedrag van de basisboete te verlagen of verhogen. Het gaat onder meer om een beoordeling van (1) de aard, de ernst en de duur van de overtreding in het specifieke geval, (2) de opzettelijke of nalatige aard van de inbreuk, (3) de genomen maatregelen om de door betrokkenen geleden schade te beperken en (4) de categorieën van persoonsgegevens waarop de inbreuk betrekking heeft. In beginsel wordt daarbij binnen de bandbreedte van de aan die overtreding gekoppelde boetecategorie gebleven. De AP kan, zo nodig en afhankelijk van de mate waarin voornoemde factoren daartoe aanleiding geven, de boetebandbreedte van de naasthogere respectievelijk de naastlagere categorie toepassen.

4.4 Boetehoogte

4.4.1 Aard, ernst en duur van de inbreuk

Ingevolge artikel 7, onder a, van de Boetebeleidsregels 2019 houdt de AP rekening met de aard, de ernst en de duur van de inbreuk. Bij de beoordeling hiervan betrekt de AP onder meer de aard, de omvang of het doel van de verwerking alsmede het aantal getroffen betrokkenen en de omvang van de door hen geleden schade.

Artikel 32 van de AVG, gelezen in samenhang met de NEN 7510 en 7513 verplichten zorgverleners tot vertrouwelijkheid en zorgvuldigheid met betrekking tot medische gegevens. Het belang van het treffen van passende beveiligingsmaatregelen is onder meer gelegen in het behoud en herstel van het vertrouwen van de patiënten in een zorgvuldige omgang van hun medische gegevens. Het beschamen daarvan heeft niet alleen een weerslag op de reputatie van de betrokken zorgverleners, maar op de gehele sector. Beveiligingsmaatregelen, zoals maatregelen met betrekking tot tweefactor authenticatie en het regelmatig controleren van de logbestanden, zijn noodzakelijke maatregelen voor behoud en herstel van dat vertrouwen.

Het HagaZiekenhuis heeft in ieder geval sinds januari 2018 geen passende beveiligingsmaatregelen getroffen die zien op tweefactor authenticatie en het regelmatig beoordelen van logbestanden. Het ziekenhuisinformatiesysteem heeft niet de ingebouwde verplichting - maar uitsluitend de mogelijkheid - om met tweefactor authenticatie in te loggen en zij controleert de logging niet regelmatig. Daardoor zijn in ieder geval gedurende deze periode niet de noodzakelijke maatregelen getroffen die zien op de bescherming van persoonsgegevens, in het bijzonder maatregelen die zien op het voorkomen en opmerken van (mogelijke) onbevoegde inzage in patiëntendossiers. De overtreding duurt daarmee op structurele wijze voor een lange periode voort, gedurende welke periode een grote groep onbevoegden toegang kan krijgen tot gezondheidsgegevens van patiënten van het HagaZiekenhuis. Des te meer in het licht van het datalek van de bekende Nederlander, waarbij het HagaZiekenhuis begin 2018 heeft geconstateerd dat een

groot aantal medewerkers onbevoegde inzage hebben gehad in een patiëntendossier, had het op de weg van het HagaZiekenhuis gelegen om de normen - die mede zien op het voorkomen van dergelijke onbevoegde inzage - te implementeren en de overtreding van artikel 32 van de AVG spoedig te beëindigen. Gelet hierop, alsmede de grote omvang van het aantal betrokken patiënten die zijn opgenomen in het ziekenhuisinformatiesysteem[29] en het type persoonsgegevens (gezondheidsgegevens), is naar het oordeel van de AP sprake van een situatie waarin dat vertrouwen in hoge mate is beschaamd. Dit acht de AP ernstig.

Voor zover de periode van de geconstateerde overtreding ziet op een gedraging van het HagaZiekenhuis onder de werking van de Wbp, is van belang dat het HagaZiekenhuis tevens onder het regime van de Wbp - gelijk aan het regime van de AVG - passende technische en organisatorische maatregelen diende te nemen om de persoonsgegevens te beveiligen.[30] Van een materiele wijziging in de bepaling is derhalve geen sprake. Bovendien is het niet naleven van dezelfde plicht onder de Wbp, weliswaar met een lagere basisboete dan onder de AVG, met dezelfde boetecategorie en daarbij behorende zelfde bandbreedte beboetbaar. Ook is naar het oordeel van de AP onder het regime van de Wbp sprake van ernstige verwijtbare nalatigheid[31] aan de zijde van het HagaZiekenhuis, nu het HagaZiekenhuis ook in deze periode heeft nagelaten maatregelen te treffen die zien op een juiste implementatie van het hanteren van tweefactor authenticatie en het regelmatig controleren van de logbestanden. Van het HagaZiekenhuis mag mede gelet op de aard en de omvang van de verwerking wel worden verwacht dat zij zich van de voor haar geldende normen vergewist. Het belang hiervan wordt versterkt door het in januari opgetreden datalek, dat mede kan worden voorkomen en opgemerkt door het treffen van dergelijke maatregelen. Gelet hierop houdt de AP wat betreft de duur van de overtreding rekening met een periode van januari 2018 tot en met heden, waarbij zij met name van belang acht dat daarmee naar het oordeel van de AP sprake is van een structurele overtreding die nog steeds voortduurt.

Gelet op de ernst van de voortdurende overtreding ziet de AP aanleiding om het basisbedrag van de boete op grond van artikel 7, aanhef en onder a, van de Boetebeleidsregels 2019 te verhogen met € 75.000,-- tot € 385.000,--.

4.4.2 Opzettelijke of nalatige aard van de inbreuk

Ingevolge artikel 7, onder b, van de Boetebeleidsregels 2019 houdt de AP rekening met de opzettelijke of nalatige aard van de inbreuk.

In het door het HagaZiekenhuis opgestelde rapport "Onderzoek onrechtmatige inzage patiëntdossier" van mei 2018 staat dat een groot aantal medewerkers een patiëntendossier onrechtmatig heeft geraadpleegd. Zij hadden geen behandel- of zorgrelatie met de patiënt. Diverse maatregelen worden aanbevolen, die

[29] In dit kader verwijst de AP naar de door het HagaZiekenhuis ter zienswijzezitting overgelegde cijfers uit het Jaarverslag. In 2017 had het HagaZiekenhuis (afgerond) 28.500 opnamen, 158.000 eerste polikliniekbezoeken, 52.000 eerste hulp consulten en 143.000 verpleegdagen.
[30] Artikel 13 van de Wbp, gelezen in samenhang met gelezen in samenhang met artikel 3, tweede lid, van het Besluit elektronische gegevensverwerking door zorgaanbieders en het bepaalde onder 9.4.1 en onder 12.4.1 van NEN 7510-2.
[31] Artikel 66, vierde lid, van de Wbp, waaruit volgt dat de AP geen bestuurlijke boete oplegt, dan nadat de AP een bindende aanwijzing heeft gegeven, tenzij de overtreding opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid.

mede zien op het doen van extra steekproeven om de naleving van de regeling te toetsen. De directie van het HagaZiekenhuis was als deelnemend lid van de Datalekcommissie op de hoogte van de onbevoegde inzage van dit patiëntendossier.[32] In het Informatiebeveiligingsbeleid wordt verwezen naar de NEN-7510 en NEN 7513, waaraan dient te worden voldaan. Nu de getroffen maatregelen niet zien op een juiste implementatie van het hanteren van tweefactor authenticatie en het regelmatig controleren van de logbestanden, doch van het HagaZiekenhuis mede gelet op de aard en de omvang van de verwerking wel mag worden verwacht dat zij zich van de voor haar geldende normen vergewist, is de AP van oordeel dat het HagaZiekenhuis in elk geval bijzonder nalatig is geweest in het treffen van dergelijke maatregelen. Daarbij neemt de AP mede in aanmerking de reactie van het HagaZiekenhuis tijdens het OTP dat zij in verband met vervolgacties vanwege voornoemd datalek geen tijd beschikbaar had voor het treffen van een beveiligingsmaatregel die ziet op het regelmatig controleren van logbestanden. Het HagaZiekenhuis is verantwoordelijk voor de invoering van structuren en middelen die zijn afgestemd op de aard en complexiteit van het ziekenhuis. Als zodanig kan zij inbreuken op de AVG niet legitimeren door een tekort aan middelen te claimen. Dat het HagaZiekenhuis in verband met het treffen van andere beveiligingsmaatregelen geen tijd beschikbaar heeft, ontslaat haar derhalve - wat daar ook van zij - niet van de verplichting ook passende beveiligingsmaatregelen te treffen die zien op het voorkomen van de voorliggende voortdurende overtreding. Evenmin de constatering van het HagaZiekenhuis dat voornoemd datalek volgens haar geen gevolg was van het feit dat tweefactor authenticatie en het regelmatig controleren van logbestanden zoals voorgesteld in haar zienswijze van 18 april 2019 nog niet volledig is ingevoerd. Daarbij merkt de AP op dat ook tweefactor authenticatie en het regelmatig controleren van logbestanden, naast de overige door het HagaZiekenhuis naar aanleiding van voornoemd datalek getroffen beveiligingsmaatregelen, zien op het voorkomen en opmerken van onbevoegde inzage in patiëntgegevens. In het licht van artikel 32, eerste lid, van de AVG dient een geheel van maatregelen te worden getroffen. Gelet op het voorgaande is de AP van oordeel dat het HagaZiekenhuis in elk geval bijzonder nalatig is geweest in het treffen van passende beveiligingsmaatregelen die zien op het hanteren van tweefactor authenticatie en het regelmatig controleren van de logbestanden.

Gelet op de nalatige aard van de inbreuk ziet de AP aanleiding om het basisbedrag van de boete op grond van artikel 7, onder b, van de Boetebeleidsregels 2019 te verhogen met € 75.000,-- tot € 460.000, -.

4.4.3 Genomen maatregelen

Ingevolge artikel 7, onder c, van de Boetebeleidsregels 2019 houdt de AP rekening met de door de verwerkingsverantwoordelijke genomen maatregelen om de door betrokkenen geleden schade te beperken.

Aan de hand van het rapport "Onderzoek onrechtmatige inzage patiëntdossier" van mei 2018 heeft het HagaZiekenhuis uit eigen initiatief een aantal beveiligingsmaatregelen aanbevolen. Deze maatregelen zagen onder meer op de bewustwording van de medewerkers, het frequenter uitvoeren van steekproeven, het inventariseren en waar nodig aanpassen van de autorisaties en het aanscherpen van het Autorisatiebeleid en de waarschuwingstekst van de noodknopprocedure. De AP heeft in haar definitieve

[32] Dit blijkt onder meer uit pag. 4 van het rapport Onderzoek onrechtmatige inzage patiëntdossier en de verklaring van [VERTROUWELIJK] Verslag van gesprekken OTP HagaZiekenhuis.

rapport van maart 2019 geconcludeerd dat het toegangscontrolebeleid van het HagaZiekenhuis voldoet aan norm NEN 7510-2. Verder heeft de AP geconcludeerd dat het HagaZiekenhuis voldoende maatregelen heeft genomen met betrekking tot de bewustwording van medewerkers ten aanzien van informatiebeveiliging. Gelet hierop heeft de AP beoordeeld dat het HagaZiekenhuis in ieder geval enkele in het rapport aanbevolen maatregelen die zien op de bescherming van patiëntgegevens in het ziekenhuisinformatiesysteem van het HagaZiekenhuis heeft getroffen.

De keerzijde hiervan is dat het rapport "Onderzoek onrechtmatige inzage patiëntdossier" expliciet meldt dat er frequenter steekproeven moeten worden gedaan die zien op het controleren van logbestanden, hetgeen het HagaZiekenhuis (nog) niet heeft opgevolgd. De reactie van het HagaZiekenhuis tijdens het OTP dat zij in verband met vervolgacties vanwege voornoemd datalek geen tijd beschikbaar had voor het treffen van een beveiligingsmaatregel die ziet op het regelmatig controleren van logbestanden , ontslaat haar gelet op het voorgaande onder paragraaf 3.3.3 niet van deze verplichting. Verder ziet het onderdeel authenticatie bij uitstek op het voorkomen van onbevoegde inzage in patiëntgegevens. Het HagaZiekenhuis heeft hier ten onrechte niet op eigen initiatief aandacht aan besteed, hetgeen des te meer voor de hand had gelegen naar aanleiding van voormeld datalek.

Nu de beveiligingsmaatregelen die zien op de bescherming van patiëntgegevens in totaliteit dienen te worden bezien, ziet de AP geen aanleiding om het basisbedrag van de boete op grond van artikel 7, onder c van de Beleidsregels 2019 te verlagen.

4.4.4 Categorieën van persoonsgegevens

Ingevolge artikel 7, onder g, van de Boetebeleidsregels 2019 houdt de AP rekening met de categorieën van persoonsgegevens waarop de inbreuk betrekking heeft.

Het HagaZiekenhuis verwerkt in grote hoeveelheid bijzondere persoonsgegevens in het ziekenhuisinformatiesysteem.[33] Het onbevoegd inzien van patiëntendossiers kan ernstige nadelige gevolgen hebben voor de bescherming van persoonsgegevens inzake de gezondheid.

Nu de categorieën van persoonsgegevens waarop de inbreuk betrekking heeft in het voorliggende geval tevens in de beoordeling van artikel 7, eerste lid, aanhef en onder a, van de Boetebeleidsregels 2019 bij de aard en ernst van de inbreuk als boeteverhogende factor is meegenomen, ziet de AP geen aanleiding om het basisbedrag van de boete tevens zelfstandig op grond van artikel 7, onder g, van de Boetebeleidsregels 2019 te verhogen.

4.4.5 Overige omstandigheden

De AP ziet geen aanleiding het basisbedrag van de boete op grond van de overige in artikel 7 van de Boetebeleidsregels 2019 genoemde omstandigheden, voor zover van toepassing in het voorliggende geval, te verhogen of te verlagen. Voor zover het HagaZiekenhuis heeft aangevoerd dat zij heeft meegewerkt met het onderzoek van de AP en direct actieplannen heeft opgesteld om de door de AP geconstateerde

[33] https://www.hagaziekenhuis.nl/over-hagaziekenhuis/verslaglegging-en-verantwoording/kerncijfers.aspx
Het aantal opnamen in 2017 was 28.498, het aantal eerste poliklinieke bezoeken 158.176 en het aantal eerste hulp consulten 52.241.

onvolkomenheden te verbeteren, is van belang dat deze medewerking niet verder gaat dan haar wettelijke plicht om te voldoen aan artikel 32, eerste lid, van de AVG. De AP ziet geen aanleiding voor het oordeel dat het HagaZiekenhuis op bijzondere wijze heeft gehandeld, waardoor de gevolgen voor de rechten van betrokkenen aanzienlijk zijn beperkt. Daarbij betrekt de AP dat het HagaZiekenhuis - ondanks voornoemd datalek en het aangekondigde onderzoek van de AP in oktober 2018 - sindsdien geen maatregelen heeft getroffen en feitelijk heeft toegepast om de overtreding op korte termijn te beëindigen.

De AP stelt het totale boetebedrag gelet op het voorgaande vast op € 460.000,--.

4.4.6 Evenredigheid

Tot slot beoordeelt de AP op grond van artikelen 3:4 en 5:46 van de Awb (evenredigheidsbeginsel) of de toepassing van haar beleid voor het bepalen van de hoogte van de boete gezien de omstandigheden van het concrete geval, niet tot een onevenredige uitkomst leidt. Toepassing geven aan het evenredigheidsbeginsel brengt volgens de Boetebeleidsregels 2019 mee dat de AP bij het vaststellen van de boete zo nodig rekening houdt met de financiële omstandigheden waarin de overtreder verkeert.

Het HagaZiekenhuis heeft ter zienswijzezitting een beroep gedaan op beperkte draagkracht, onderbouwd met de concept jaarrekening 2018. In dat kader voert zij aan dat het HagaZiekenhuis in 2018 [VERTROUWELIJK] heeft overgehouden ten gevolge van incidentele baten. De AP ziet hierin geen aanleiding om aan te nemen dat het HagaZiekenhuis een boete van € 460.000,-- gezien haar financiële positie niet zou kunnen dragen.

4.4.7 Conclusie

De AP stelt het totale boetebedrag vast op € 460.000,--.

5. Last onder dwangsom

5.1 Aanleiding

Nu het gaat om een voortdurende overtreding van artikel 32, eerste lid, van de AVG, dient deze zo spoedig mogelijk te worden beëindigd. Om die reden legt de AP naast voornoemde boete een last onder dwangsom op op grond van artikel 58, tweede lid, aanhef en onder d, van de AP, artikel 16, eerste lid, van de UAVG en artikel 5:32, eerste lid, van de Awb.

5.2 Begunstigingstermijn en hoogte dwangsom

De AP verbindt aan de last onder dwangsom een begunstigingstermijn van **vijftien weken**. Bij het vaststellen van deze termijn heeft zij rekening gehouden met de planning die ziet op de voorgenomen maatregelen zoals opgenomen in de zienswijze van het HagaZiekenhuis van 18 april 2019. Ter zienswijzezitting heeft het HagaZiekenhuis toegelicht dat de uitvoering van de maatregelen zoals opgenomen in haar planning in haar macht liggen en dat de planning realistisch is. Hoewel de planning zoals opgesteld door het HagaZiekenhuis tevens uitgaat van een controle van logbestanden binnen het

autorisatieprofiel van zes (al dan niet reguliere) patiëntendossiers en dit vanwege de zeer beperkte omvang naar het oordeel van de AP gelet op het voorgaande niet tot het vereiste passende beveiligingsniveau leidt, ziet de AP niet in dat het HagaZiekenhuis niet binnen deze begunstigingstermijn ook op dit punt kan voldoen aan artikel 32, eerste lid, van de AVG. Daarbij is van belang dat de planning wel een wekelijkse (handmatige) controle van de logging van alle patiëntendossiers die - buiten het autorisatieprofiel - zijn geraadpleegd via de noodknopprocedure omvat. Niet valt in te zien dat zij niet binnen de begunstigingstermijn ook ten aanzien van de controle van logbestanden binnen het autorisatieprofiel kan voldoen aan artikel 32, eerste lid, van de AVG. Daarbij is niet vereist dat de controle van de logging ziet op alle patiëntendossiers die binnen het autorisatieprofiel zijn geraadpleegd, doch dat de controle zodanig wordt ingeregeld dat gevallen van onrechtmatige verwerkingen die plaatsvinden binnen de autorisatie in voldoende mate kunnen worden gedetecteerd. Nu de vraag of op dit punt wordt voldaan aan artikel 32, eerste lid, van de AVG afhankelijk is van de wijze waarop controle plaatsvindt - bijvoorbeeld aan de hand van een profiel van indicaties dat zij hanteert om onrechtmatige toegang op te merken - en het geheel van beveiligingsmaatregelen in dat kader dient te worden bezien, kan de AP de omvang van een vereiste regelmatige controle van de logbestanden niet op voorhand duiden. Het HagaZiekenhuis dient derhalve toe te lichten hoe de (beoogde) controle volgens het HagaZiekenhuis in haar geval tot een aanvaardbaar niveau bijdraagt aan de signalering van onrechtmatige inzage of gebruik van patiëntgegevens binnen de autorisatieprofielen.

Artikel 5:32b, derde lid, van de Awb schrijft voor dat de dwangsombedragen in redelijke verhouding staan tot de zwaarte van het geschonden belang en tot de beoogde werking van de dwangsom. Bij dat laatste is van belang dat van een dwangsom een zodanige prikkel moet uitgaan dat aan de last wordt voldaan.

Indien het HagaZiekenhuis de geconstateerde overtreding niet binnen **vijftien weken** beëindigt, verbeurt zij na afloop van die begunstigingstermijn voor iedere twee weken dat niet (geheel) aan de last is voldaan een dwangsom. De AP stelt de hoogte van deze dwangsom voor iedere twee weken na afloop van de begunstigingstermijn vast op een bedrag van **€ 100.000,--** (zegge: honderdduizend euro), tot een maximumbedrag van in totaal **€ 300.000,--** (zegge: driehonderdduizend euro).

Indien het HagaZiekenhuis het verbeuren van de dwangsom direct na afloop van de begunstigingstermijn wenst te voorkomen, raadt de AP het HagaZiekenhuis aan om de stukken - waarmee het HagaZiekenhuis kan aantonen dat zij voldoet aan de last onder dwangsom - tijdig, doch uiterlijk een week voor het einde van de begunstigingstermijn aan de AP ter beoordeling toe te sturen.

6. Dictum

Boete

De AP legt aan het HagaZiekenhuis, wegens overtreding van artikel 32, eerste lid, van de AVG, gelezen in samenhang met artikel 3, tweede lid, Besluit elektronische gegevensverwerking door zorgaanbieders en het bepaalde onder 9.4.1 en onder 12.4.1 van NEN 7510 -2, een bestuurlijke boete op ten bedrage van

€ 460.000,-- (zegge: vierhonderdzestigduizend euro).[34]

Last onder dwangsom

Het HagaZiekenhuis dient binnen vijftien weken na dagtekening en met inachtneming van dit besluit in het kader van de gegevensverwerking in het ziekenhuisinformatiesysteem van het HagaZiekenhuis, toegankelijk voor haar medewerkers, maatregelen te nemen die ertoe leiden dat:
1. deze toegang uitsluitend mogelijk is met toepassing van tweefactor authenticatie;
2. de logbestanden regelmatig worden gecontroleerd op onrechtmatige toegang of onrechtmatig gebruik van patiëntgegevens.

Indien het HagaZiekenhuis niet uiterlijk binnen vijftien weken na datum van dit besluit de maatregelen heeft uitgevoerd om (geheel) aan de last te voldoen, verbeurt het HagaZiekenhuis een dwangsom van **€ 100.000**,-- (zegge: honderdduizend euro) voor iedere twee weken na afloop van de begunstigingstermijn, tot een maximumbedrag van in totaal **€ 300.000,--** (zegge: driehonderdduizend euro).

Hoogachtend,
Autoriteit Persoonsgegevens,

w.g.

mr. A. Wolfsen
Voorzitter

Rechtsmiddelenclausule
Indien u het niet eens bent met dit besluit kunt u binnen zes weken na de datum van verzending van het besluit digitaal of op papier een bezwaarschrift indienen bij de Autoriteit Persoonsgegevens. Voor het indienen van digitaal bezwaar, zie www.autoriteitpersoonsgegevens.nl, onder het kopje Bezwaar maken tegen een besluit, onderaan de pagina onder de kop Contact met de Autoriteit Persoonsgegevens. Het adres voor het indienen op papier is: Autoriteit Persoonsgegevens, postbus 93374, 2509 AJ Den Haag. Vermeld op de envelop 'Awb-bezwaar' en zet in de titel van uw brief 'bezwaarschrift'.
Schrijf in uw bezwaarschrift ten minste:
- uw naam en adres;
- de datum van uw bezwaarschrift;
- het in deze brief genoemde kenmerk (zaaknummer); of een kopie van dit besluit bijvoegen;
- de reden(en) waarom u het niet eens bent met dit besluit;
- uw handtekening.

[34] De AP zal voornoemde vordering uit handen geven aan het Centraal Justitieel Incassobureau (CJIB).