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

Vertrouwelijk/Aangetekend
Stichting OLVG
T.a.v. de heer prof. Dr. M.A.A.J. van den Bosch
Voorzitter Raad van Bestuur
Postbus 95500
1090 HM Amsterdam

Datum
26 november 2020

Ons kenmerk
[VERTROUWELIJK]

Contactpersoon
[VERTROUWELIJK]

Onderwerp
Besluit tot het opleggen van een bestuurlijke boete

Geachte heer Van den Bosch,

De Autoriteit Persoonsgegevens (AP) heeft besloten aan Stichting OLVG (OLVG) een **bestuurlijke boete** van **€440.000,-** op te leggen, omdat OLVG niet heeft voldaan aan het vereiste van tweefactor authenticatie en het regelmatig beoordelen van logbestanden. Daarmee heeft OLVG onvoldoende passende maatregelen genomen als bedoeld in artikel 32, eerste lid, van de Algemene Verordening Gegevensbescherming (AVG).

Hierna wordt het besluit nader toegelicht. Hoofdstuk 1 betreft een inleiding en hoofdstuk 2 beschrijft het wettelijk kader. In hoofdstuk 3 beoordeelt de AP de verwerkingsverantwoordelijkheid en de overtreding. In hoofdstuk 4 wordt de (hoogte van de) bestuurlijke boete uitgewerkt en hoofdstuk 5 bevat het dictum en de rechtsmiddelenclausule.

Datum
26 november 2020

Ons kenmerk
[VERTROUWELIJK]

1. Inleiding

1.1 Betrokken rechtspersonen en aanleiding onderzoek

OLVG is een stichting die statutair is gevestigd op Oosterpark 9, te Amsterdam. OLVG is ingeschreven in het handelsregister van de Kamer van Koophandel onder het nummer 41199082. OLVG is een topklinisch opleidingsziekenhuis in Amsterdam met twee hoofdlocaties in Amsterdam-Oost en -West. OLVG biedt medische zorg aan jaarlijks circa 500.000 patiënten. In 2018 had OLVG 5890 medewerkers in loondienst, waarvan 4274 in patiëntgebonden functies.[1]

De AP heeft twee datalekmeldingen ontvangen van Stichting OLVG over inzage door medewerkers en werkstudenten in elektronische patiëntendossiers. Naar aanleiding van deze datalekmeldingen is de AP een ambtshalve onderzoek gestart naar de naleving door OLVG van artikel 32, eerste lid, van de AVG door onder andere beveiligingsaspecten zoals de authenticatie en de controle van de logging te onderzoeken.

1.2 Procesverloop

Bij brief van 17 april 2019 heeft de AP het onderzoek aangekondigd en vragen gesteld aan OLVG. Deze vragen zijn bij brief van 3 mei 2019 door OLVG beantwoord.

Op 22 mei 2019 hebben vijf toezichthouders van de AP een onderzoek ter plaatse verricht bij OLVG, locatie Oost, aan de Oosterpark 9 te Amsterdam. Tijdens dit onderzoek is het ziekenhuisinformatiesysteem op verschillende momenten en onderdelen gedemonstreerd en ingezien. Tevens zijn er mondelinge verklaringen afgenomen van leden van de Raad van Bestuur en van verschillende medewerkers van OLVG.

De AP heeft op 10 februari 2020 het rapport met bevindingen aan OLVG verstuurd. Bij brief van 17 februari 2020 heef de AP aan OLVG een voornemen tot handhaving verzonden. Daartoe tevens bij deze brief door de AP in de gelegenheid gesteld, heeft OLVG op 27 maart 2020 schriftelijk en op 25 juni 2020 mondeling haar zienswijze gegeven over dit voornemen en het daaraan ten grondslag gelegde rapport.

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, van de AVG is deze verordening van toepassing op de verwerking van

[1] Jaarverantwoording 2018 OLVG, p. 5-6.

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 van de AVG 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

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 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.

2.3 Bestuurlijke boete

Ingevolge artikel 58, tweede lid, aanhef en onder i, in samenhang met artikel 83, vierde lid, aanhef en onder a, van de AVG en artikel 14, derde lid, van de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) is de AP bevoegd om ten aanzien van inbreuken op de AVG een bestuurlijke boete op te leggen.

2.3.1 AVG

Ingevolge artikel 83, eerste lid, van de AVG 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 van de AVG 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 UAVG

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

3.Beoordeling

3.1 Verwerking van persoonsgegevens

OLVG gebruikt sinds 19 oktober 2015 een nieuw en geïntegreerd ziekenhuisinformatiesysteem waarin elektronisch patiëntendossiers opgeslagen zijn.[2] De gegevens over patiënten die OLVG in het ziekenhuisinformatiesysteem verwerkt is informatie waarmee OLVG natuurlijke personen kan identificeren. Deze patiëntgegevens zijn daarom persoonsgegevens in de zin van artikel 4, onderdeel 1, van de AVG. Een deel van deze gegevens zijn gezondheidsgegevens en zijn derhalve ook te kwalificeren als een bijzondere categorie van persoonsgegevens in de zin van artikel 9 van de AVG.

Voorts is sprake van een verwerking van persoonsgegevens in de zin van artikel 4, onderdeel 2, van de AVG. Door zijn reikwijdte omvat het begrip 'verwerking' elke mogelijke bewerking of geheel van bewerkingen van persoonsgegevens. Het vastleggen en raadplegen van patiëntgegevens in het ziekenhuisinformatiesysteem valt daar ook onder. Het betreft een omvangrijke verwerking waarbij veel mensen betrokken zijn. Zo heeft OLVG in 2018 alleen al aan circa 500.000 patiënten medische zorg verleend.[3]

3.2 Verwerkingsverantwoordelijke

In het kader van de vraag of OLVG in strijd handelt met artikel 32, eerste lid, van de AVG, is ook van belang om te bepalen wie aan te merken is als verwerkingsverantwoordelijke als bedoeld in artikel 4, onderdeel 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 OLVG - vaststelt. Om deze vraag te beantwoorden hecht de AP in dit geval waarde aan de verklaringen van het bestuur van OLVG tijdens het onderzoek ter plaatse, de inschrijving in het handelsregister van de Kamer van Koophandel, beleidsstukken en de jaarverantwoordingen van OLVG van 2015 en 2018.

[2] Onderzoek ter plaatse d.d. 22 mei 2019, Verslag 1: vraag 1.; Verslag 2: figuur 2 t/m 7; Jaarverantwoording 2015 Stichting OLVG, p.16, 17; Gespreksverslag zienswijzezitting d.d. 25 juni 2020, p. 6.
[3] Jaarverantwoording 2018 OLVG, p. 5-6.
https://www.olvg.nl/sites/default/files/jaarverantwoording_2018_olvg_gewaarmerkt_dig_1.pdf

De voorzitter van de Raad van Bestuur van OLVG heeft verklaard dat in 2013 een bestuurlijke fusie heeft plaatsgevonden tussen stichting Sint Lucas Andreas Ziekenhuis en stichting Onze Lieve Vrouwen Gasthuis en dat er sindsdien één gezamenlijk bestuur is.[4] Vervolgens zijn deze twee ziekenhuizen in juni 2015 juridisch gefuseerd tot één ziekenhuis, genaamd: Stichting OLVG.[5] Verder is tijdens de fusie in 2015 het huidige ziekenhuisinformatiesysteem uniform binnen OLVG geïntroduceerd.[6] Dit systeem is zoals hiervoor vermeld uiteindelijk op 19 oktober 2015 in gebruik genomen door OLVG.[7]

Volgens de inschrijving in de Kamer van Koophandel zijn de activiteiten van OLVG 'algemene ziekenhuizen, praktijken van medisch specialisten en medische dagbehandelcentra, gezondheidscentra en ambulante jeugdzorg.'[8] OLVG noemt verder in haar informatiebeveiligings- & privacybeleid dat het stelsel van beveiligings- en privacy maatregelen zich onder andere richt op het beveiligen van alle informatie en informatiesystemen, het voorkomen van informatiebeveiligingsincidenten en het nemen van voorzorgsmaatregelen. Het informatiebeveiligings- & privacybeleid is van toepassing op alle bedrijfsonderdelen van het OLVG en op de gegevensuitwisseling met andere organisaties.[9] Ook uit de 'regeling patiëntgegevens en gebruik communicatiemiddelen' blijkt dat OLVG heeft bepaald hoe medewerkers van OLVG om moeten gaan met elektronische patiëntendossiers.[10]

De AP constateert op grond van bovengenoemde stukken en verklaringen van het bestuur van OLVG dat OLVG het doel en de middelen vaststelt voor de verwerking van persoonsgegevens ten behoeve van de elektronische patiëntendossiers van OLVG. Dat betekent dat OLVG verwerkingsverantwoordelijke is in de zin van artikel 4, onderdeel 7, van de AVG voor de verwerking van patiëntgegevens in het ziekenhuisinformatiesysteem van OLVG.

3.3 Overtreding inzake gegevensbeveiliging

3.3.1 Inleiding

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

[4] Onderzoek ter plaatse d.d. 22 mei 2019, Verslag 1:Raad van Bestuur, vraag 1.
[5] Jaarverantwoording 2015 OLVG, beschikbaar via: https://www.olvg.nl/sites/default/files/jaarverantwoording_2015.pdf, p. 4, laatst geraadpleegd op: 30 juli 2019. Tevens: onderzoek ter plaatse d.d. 22 mei 2019, Verslag 1:Raad van Bestuur, vraag 1. Ook heeft OLVG twee buitenpoliklinieken in Amsterdam, zie uittreksel KvK: 41199082 onder vestigingen.
[6] Onderzoek ter plaatse d.d. 22 mei 2019, Verslag 1:Raad van Bestuur, vraag 1; Jaarverantwoording 2015 OLVG, beschikbaar via: https://www.olvg.nl/sites/default/files/jaarverantwoording_2015.pdf, p. 4, laatst geraadpleegd op: 30 juli 2019.
[7] "In oktober 2015 is het gezamenlijke elektronische patiëntendossier (Epic) live gegaan."; Jaarverantwoording 2015 OLVG, beschikbaar via: https://www.olvg.nl/sites/default/files/jaarverantwoording_2015.pdf, p. 17, laatst geraadpleegd op: 30 juli 2019; en artikel: https://www.medicalfacts.nl/2015/11/03/olvg-neemt-elektronisch-patientendossier-epic-in-gebruik/. Gespreksverslag zienswijzezitting d.d. 25 juni 2020, p. 6.
[8] OLVG Oost is de hoofdvestiging. Andere vestigingen zijn OLVG West , Jan Tooropstraat 164, 1061 AE in Amsterdam en de buitenpoli's OLVG IJburg en OLVG Spuistraat. (uittreksel uit de het handelsregister van de Kamer van Koophandel van 25 maart 2019.
[9] Reactie OLVG op informatieverzoek AP d.d. 3 mei 2019, bijlage 8.
[10] Reactie OLVG op informatieverzoek AP d.d. 3 mei 2019, bijlage 28.

van de techniek en de uitvoeringskosten afgezet tegen de risico's en de aard van de te beschermen persoonsgegevens.[11] De AP toetst in het navolgende of OLVG een passend beveiligingsniveau heeft gehanteerd voor de verwerking van persoonsgegevens in haar ziekenhuisinformatiesysteem.

3.3.2 Tweefactor authenticatie

3.3.2.1 Feiten

Het huidige ziekenhuisinformatiesysteem is op 19 oktober 2015 door OLVG in gebruik genomen. Tijdens het onderzoek ter plaatse op 22 mei 2019 bij OLVG hebben toezichthouders van de AP onderzocht op welke wijze medewerkers van OLVG toegang verkrijgen tot de elektronische patiëntendossiers (inloggen) binnen het ziekenhuisinformatiesysteem. De AP constateert dat de authenticatie van de identiteit van de medewerker voor het gebruik van het ziekenhuisinformatiesysteem van OLVG op twee manieren mogelijk is, afhankelijk of toegang wordt gevraagd van binnen of van buiten het OLVG-netwerk.

De toezichthouders van de AP hebben tijdens dit het onderzoek ter plaatse[12] vastgesteld dat medewerkers van OLVG op een computer(-terminal) *binnen* het OLVG-netwerk kunnen inloggen op de virtuele werkplek (VDI).[13] Het inloggen gebeurt middels het invoeren van een gebruikersnaam en wachtwoord en daarbij wordt géén gebruik gemaakt van een personeelspas of een token als onderdeel van het inlogproces om toegang te krijgen tot het ziekenhuisinformatiesysteem. Deze manier van inloggen is op verschillende momenten tijdens het onderzoek ter plaatse geconstateerd. De toezichthouders van de AP hebben dit allereerst geconstateerd tijdens de demonstratie van het ziekenhuisinformatiesysteem.[14] Deze constatering is mede bevestigd door de mondelinge verklaringen van [VERTROUWELIJK].[15]

Voorts hebben de toezichthouders van de AP tijdens controles op de werkplek van drie verschillende medewerkers[16] van OLVG geconstateerd dat indien de medewerker zijn/haar gebruiksnaam en wachtwoord correct invult, hij/zij toegang krijgt tot de VDI-omgeving en tot de elektronische patiëntendossiers. Het bleek dat hierbij sprake is van een 'single sign on' functionaliteit[17], waardoor de medewerker die is ingelogd op de VDI ook meteen toegang heeft tot het ziekenhuisinformatiesysteem met de elektronische patiëntendossiers.

Voorts wordt vermeld in artikel 2.1. van de 'Regeling patiëntgegevens en gebruik communicatiemiddelen' dat "*medewerkers van OLVG, (...) voor zover dit nodig is voor de functie die zij binnen OLVG uitoefenen, door middel van inlogcode en wachtwoord toegang [wordt] verleend tot het elektronisch patiëntendossier in Epic en vergelijkbare patiënteninformatiesystemen binnen OLVG (hierna samen genoemd "EPD").*"[18]

[11] Overweging 83 van de AVG.
[12] Onderzoek ter plaatse d.d. 22 mei 2019, Verslag 2, 6, 7 en 8.
[13] Virtual Desktop Infrastructure.
[14] Onderzoek ter plaatse d.d. 22 mei 2019, Verslag 2: vraag 1 t/m 4 en figuur 1 t/m 7. Demonstratie door [VERTROUWELIJK] van OLVG.
[15] Onderzoek ter plaatse d.d. 22 mei 2019, Verslag 2: vraag 1 en 2. En Onderzoek ter plaatse d.d. 22 mei 2019, Verslag 2: vraag 2 en 3.
[16] Controle op de werkplek van [VERTROUWELIJK] (verslag 6), een [VERTROUWELIJK] (verslag 7) en een [VERTROUWELIJK] (verslag 8).
[17] Onderzoek ter plaatse d.d. 22 mei 2019, verslag 7 en 8, niet bij de [VERTROUWELIJK] (verslag 6). Zie ook de verklaring van [VERTROUWELIJK] van OLVG, onderzoek ter plaatse d.d. 22 mei 2019, Verslag 2: vraag 2 en 3.
[18] Reactie OLVG op informatieverzoek AP d.d. 3 mei 2019, bijlage 28. Op dit document staat dat het vanaf 25 mei 2018 van kracht is.

De tweede manier om toegang te krijgen tot het ziekenhuisinformatiesysteem is via een computer *buiten* het OLVG-netwerk. Tijdens de demonstratie tijdens het onderzoek ter plaatse heeft de AP geconstateerd dat ook kan worden ingelogd op de VDI via een computer *buiten* het OLVG-netwerk, bijvoorbeeld wanneer medewerkers thuiswerken.[19] In dit geval dient te worden ingelogd in de VDI omgeving en het ziekenhuisinformatiesysteem met een gebruikersnaam en wachtwoord[20] in combinatie met een wisselende token die wordt ontvangen c.q. aangemaakt per sms of applicatie.[21]

OLVG heeft op 9 maart 2020 aan elke computer(-terminal) een reader gekoppeld en daarmee de bovenstaande werkwijze veranderd. Hierdoor moet een medewerker zijn/haar personeelspas voor deze reader houden en vervolgens een wachtwoord invoeren voordat toegang tot de computer kan worden verkregen.[22]

3.3.2.2 Beoordeling

Op grond van artikel 32, eerste lid, van de AVG dient de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen te treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. Bij de beoordeling van de risico's dient volgens artikel 32, tweede lid, van de AVG aandacht te worden besteed aan risico's die zich voordoen bij de verwerking van persoonsgegevens. Naarmate de gegevens een gevoeliger karakter hebben, of de context waarin zij worden gebruikt een grotere bedreiging vormt voor de persoonlijke levenssfeer van betrokkenen, worden er zwaardere eisen gesteld aan de beveiliging van gegevens.

OLVG verwerkt in haar ziekenhuissysteem op grote schaal persoonsgegevens van circa 500.000 patiënten. Het gaat (veelal) om uiterst gevoelige gegevens over de gezondheid. Gegevens over de gezondheid zijn op grond van artikel 9, eerste lid, van de AVG aangemerkt als een bijzondere categorie van persoonsgegevens. Deze persoonsgegevens die door hun aard bijzonder gevoelig zijn wat betreft de grondrechten en fundamentele vrijheden, verdienen specifieke bescherming aangezien de context van de verwerking ervan significante risico's kan meebrengen voor de grondrechten en de fundamentele vrijheden. OLVG dient daarom passende maatregelen te nemen om persoonsgegevens zo goed mogelijk te beschermen en inbreuken zoveel als mogelijk te voorkomen.

Gezien de gevoelige aard van de gegevens, de grote omvang van de verwerking door OLVG en de risico's voor de persoonlijke levenssfeer van betrokkenen had OLVG bij de toegang tot persoonsgegevens in elektronische patiëntendossiers een tweefactor authenticatie moeten inregelen. De AP heeft in het voorgaande echter vastgesteld dat medewerkers op een computer binnen het OLVG-netwerk toegang konden krijgen tot de gegevens in de elektronische patiëntdossiers met alleen iets wat een medewerker weet (namelijk een gebruikersnaam en wachtwoord). Dat betekent dat in dat geval gebruik werd gemaakt van slechts één factor. Op grond van het onderzoek is gebleken dat OLVG géén gebruik heeft gemaakt van een pas, token of een andere tweede factor. Daarmee heeft OLVG niet aan het vereiste van minimaal

[19] Onderzoek ter plaatse d.d. 22 mei 2019, Verslag 2: authenticatie, vraag 4.
[20] Onderzoek ter plaatse d.d. 22 mei 2019, Verslag 2: figuur 7 portal.olvg.nl.
[21] Onderzoek ter plaatse d.d. 22 mei 2019, Verslag 2: authenticatie, vraag 4, figuur 7-13.
[22] Schriftelijke zienswijze OLVG, 27 maart 2020, p. 24 en 25. Mondelinge zienswijze OLVG, 25 juni 2020, p. 4.

tweefactor authenticatie voldaan, wat in de context van deze verwerking in het kader van artikel 32 van de AVG wel is vereist. Een dergelijke beveiligingsmaatregel acht de AP, ook gezien de huidige stand van de techniek en de uitvoeringskosten, passend. Daarbij neemt de AP in aanmerking dat algemeen geaccepteerde beveiligingsstandaarden, zoals de Nederlandse norm voor informatiebeveiliging in de zorg, tweefactor authenticatie voorschrijven.

OLVG heeft verder in haar Informatiebeveiligings- & privacybeleid aangegeven dat voornoemd beleid is gebaseerd op: 1) de Nederlandse norm voor informatiebeveiliging in de zorg, te weten: NEN 7510, NEN 7512 en NEN 7513 en 2) de actuele wet- en regelgeving, waaronder de AVG. OLVG streeft ernaar aantoonbaar te voldoen aan deze normen.[23] OLVG heeft zich aldus ook zelfstandig gecommitteerd te voldoen aan bovenstaande NEN-normen, waarin is vastgesteld dat de identiteit van gebruikers moet worden vastgesteld door middel van tweefactor authenticatie.[24]

Ten overvloede merkt de AP tot slot op dat specifiek ten aanzien van de bewoordingen 'passende technische en organisatorische maatregelen' - zoals opgenomen in artikel 32 AVG - sprake is van een voortzetting van wat ook al gold onder Richtlijn 95/46/EG en de Wet bescherming persoonsgegevens (Wbp).[25] Van een materiële wijziging is geen sprake. Onder die omstandigheden ligt het voor de hand — ook met het oog op de rechtszekerheid — de in het verleden gevolgde invulling voort te zetten bij de uitleg van artikel 32, eerste lid, van de AVG. Dat betekent dat de reeds in het verleden gebezigde invulling via de in de NEN-normen vervatte eisen van tweefactor authenticatie en het regelmatig beoordelen van de logbestanden wordt gehandhaafd.[26] Door de AP is ook steeds duidelijk uitgedragen dat de NEN 7510, als algemeen geaccepteerde beveiligingsstandaard binnen de praktijk van de informatiebeveiliging in de zorg, onder het AVG-regime een belangrijke norm voor informatiebeveiliging in de zorg blijft en deze richtlijnen gevolgd moeten worden.[27]

Zienswijze OLVG en reactie AP
OLVG stelt in haar zienswijze dat de AP ten onrechte oordeelt dat OLVG geen tweefactor authenticatie heeft toegepast. Volgens Norm 9.4.1 van NEN 7510-2 (2017) behoren gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, de identiteit van gebruikers vast te stellen en dit behoort te worden gedaan door middel van authenticatie waarbij ten minste twee factoren betrokken worden. Volgens OLVG geldt al jaren dat toegang tot PC's beperkt wordt door de toegang tot de fysieke ruimte waar de PC staat. PC's staan namelijk in ruimtes waartoe men alleen toegang heeft met een persoonsgebonden personeelspas. De pas wordt zodanig geconfigureerd dat een medewerker slechts

[23] Reactie OLVG op informatieverzoek AP d.d. 3 mei 2019, bijlage 2, onder 3.3 en bijlage 8 onder 2.2.
[24] Overigens zijn zorgaanbieders op grond van artikel 3 en 5 van het Besluit elektronische gegevensverwerking door zorgaanbieders verplicht om overeenkomstig NEN 7510 en NEN 7512 zorg te dragen voor een veilig en zorgvuldig gebruik van elektronische uitwisselsystemen en dat logging voldoet aan het bepaalde in NEN 7513.
[25] Artikel 13 Wbp en artikel 17, eerste lid, Richtlijn 95/46/EG kende ook al de terminologie 'passende en organisatorische maatregelen' ter voorkoming van verlies of onrechtmatige verwerking.
[26] Zo volgt uit het rapport 'toegang tot digitale patiëntendossiers binnen zorginstellingen' van juni 2013; https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/rap_2013-patientendossiers-binnen-zorginstellingen.pdf.
[27] Vgl.: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/gezondheid/zorgverleners-en-de-avg; Zie ook communicatie door AVG helpdesk Zorg op https://www.avghelpdeskzorg.nl/onderwerpen/beveiliging/nen-7510.

toegang heeft tot ruimten en functies waarvoor de medewerker geautoriseerd is. Volgens OLVG is er geen principieel verschil tussen de toegang die beperkt is tot degene die een pas voor een reader houdt die zich bij de PC bevindt.

De AP volgt de zienswijze van OLVG niet. Voor een passende beveiliging van de persoonsgegevens in elektronische patiëntendossiers is het noodzakelijk dat het informatiesysteem van OLVG alleen met een tweefactor authenticatie toegankelijk is. Indien de toegang tot de ruimte belast is met een authenticatie via een persoonlijke pas maar de computer zelf niet met een tweefactor authenticatie, dan is de kans groter dat medewerkers die wel bevoegd zijn tot de ruimte (zoals schoonmakers) maar niet tot de elektronische patiëntendossiers, toegang kunnen krijgen tot deze dossiers. Daarnaast zijn bepaalde gedeeltes van het ziekenhuis, zoals poliklinieken, niet geheel afgesloten. Er is dus wel degelijk een belangrijk verschil met de toegang die beperkt is tot degene die een pas voor een reader houdt die zich bij de computer bevindt.
Tot slot benadrukt de AP dat norm 9.4.1 van NEN 7510-2 (2017) de term 'gezondheidsinformatiesystemen' bevat. Oftewel, de informatiesystemen zelf moeten beveiligd zijn met een tweefactor authenticatie.

Gelet op het voorgaande is de AP van oordeel dat OLVG in ieder geval tot 22 mei 2019 artikel 32, eerste lid, van de AVG heeft overtreden, nu het ziekenhuisinformatiesysteem van OLVG niet heeft voldaan aan het vereiste van tweefactor authenticatie. OLVG heeft inmiddels deze overtreding beëindigd door aan elke computer(-terminal) een reader te koppelen. Hierdoor moet een medewerker zijn/haar personeelspas voor deze reader houden en vervolgens een wachtwoord invoeren voordat toegang tot de computer kan worden verkregen.

3.3.3 Controle op logging

3.3.3.1 Feiten

In het Informatiebeveiligings- & privacybeleid van OLVG staat vermeld dat OLVG ernaar streeft aantoonbaar te voldoen aan de normen NEN 7510 (informatiebeveiliging in de zorg), NEN 7512 (vertrouwensbasis voor gegevensuitwisseling), NEN 7513 (logging acties op elektronische patiëntendossiers) en de AVG.[28] Bovendien geeft OLVG in het Logging beleid Epic aan dat dit document moet leiden tot compliance aan de norm NEN 7513 en geldende wet- en regelgeving.[29] In het Logging beleid Epic is als uitgangspunt opgenomen dat de logbestanden periodiek worden gecontroleerd op indicaties van onregelmatigheden of fouten zodat deze waar nodig bij voorkeur vroegtijdig kunnen worden ondervangen.[30] Daartoe worden alle activiteiten van gebruikers, systemen en informatiebeveiligingsgebeurtenissen in logbestanden vastgelegd.[31] Van afwijkende gebeurtenissen geregistreerd in de loggegevens wordt een rapportage opgemaakt en indien noodzakelijk wordt er nader onderzoek gedaan.[32] Het Logging beleid Epic maakt onderscheid in de wijze waarop de loggegevens worden gecontroleerd, namelijk steekproefsgewijs en op incidentbasis.[33]

[28] Onderzoek van 10 februari 2020, bijlage 2, onder 3.3 en bijlage 8 onder 2.2.
[29] Onderzoek van 10 februari 2020, bijlage 13, onder 2.1.
[30] Onderzoek van 10 februari 2020, bijlage 13, onder 4.4.
[31] Onderzoek van 10 februari 2020, bijlage 13, onder 4.2.
[32] Onderzoek van 10 februari 2020, bijlage 13, onder 4.7.
[33] Onderzoek van 10 februari 2020, bijlage 13, onder 4.6.

Op grond van het Logging beleid Epic moet voor de steekproefsgewijze controles elke vier weken een representatieve steekproef genomen worden om te analyseren.[34] Uit de Logging procedure Epic blijkt dat maandelijks een rapportage uit het datawarehouse verkregen wordt van het aantal break-the-glass-events.[35] Er zal altijd een gemiddelde hoeveelheid events zijn.[36] De EPD Dienst doet steekproefsgewijs controle van de break-the-glass-events en daarbij is zij vrij in het bepalen wat een representatieve steekproef is.[37] Indien er grote afwijkingen zijn voor één of meerdere gebruikers, dan moet er nader onderzoek gedaan worden naar deze afwijkingen.[38] De incidentele controle vindt plaats wanneer de actualiteit (vanuit een incident of een verzoek van een patiënt) hiertoe aanleiding geeft.[39] Dan zullen de nodige analyses uitgevoerd worden. Hierbij geldt dat, indien er sprake is van een verzoek van een patiënt, de vraagstelling tot onderzoek moet komen vanuit Juridische Zaken.[40] Van afwijkende gebeurtenissen worden rapporten opgemaakt.[41] In de rapportage wordt weergegeven wat de opvallende gebeurtenissen zijn en op welke manier of waarom deze gebeurtenissen opvallen, en hoe deze strijdig zijn met het beleid en/of de rechtmatige toegang tot een dossier.[42]

[VERTROUWELIJK] van OLVG heeft tijdens het onderzoek ter plaatse verklaard dat elke handeling wordt gelogd.[43] [VERTROUWELIJK] van OLVG heeft verklaard dat er ten aanzien van de controle op de logging een aantal steekproeven en incidentele controles gedaan zijn.[44] Zo is er op 26 maart 2018 een steekproef gedaan naar het break-the-glass gedrag van bepaalde functiegroepen.[45] Dit zag op de functiegroepen verpleegkundigen en artsen in opleiding en besloeg een periode van drie maanden.[46] De rapportage die opgesteld is naar aanleiding van deze steekproef bestaat uit één bladzijde met cijfers en een grafiek van het totaal aantal break-the-glass per maand, zonder analyse van voornoemde cijfers.[47]

Op 13 maart 2019 is er ook een rapport opgemaakt met daarin de analyse van de steekproef naar break-the-glass gebruik door werkstudenten.[48] De rapportage van de analyse bestaat uit acht bladzijden met een cijfermatig overzicht en analyse op afwijkend break-the-glass gebruik in de periode van 1 januari 2018 tot en met 7 februari 2019 van alle 181 werkstudenten die bij OLVG op 6 februari 2019 nog in dienst waren.[49]

[34] Onderzoek van 10 februari 2020, bijlage 13, onder 4.6.
[35] Onderzoek van 10 februari 2020, bijlage 14, onder 3.4.
[36] Onderzoek van 10 februari 2020, bijlage 14, onder 3.4.
[37] Onderzoek van 10 februari 2020, bijlage 14, onder 3.4.
[38] Onderzoek van 10 februari 2020, bijlage 14, onder 3.4.
[39] Onderzoek van 10 februari 2020, bijlage 13, onder 4.6.
[40] Onderzoek van 10 februari 2020, bijlage 13, onder 4.6.
[41] Onderzoek van 10 februari 2020, bijlage 14, onder 3.5.
[42] Onderzoek van 10 februari 2020, bijlage 14, onder 3.5.
[43] Onderzoek ter plaatse van 22 mei 2019, gespreksverslag 4, onder 1.
[44] Onderzoek ter plaatse van 22 mei 2019, gespreksverslag 4, onder 5.
[45] Onderzoek ter plaatse van 22 mei 2019, gespreksverslag 4, onder 5.
[46] Onderzoek ter plaatse van 22 mei 2019, gespreksverslag 4, onder 7.
[47] Onderzoek van 10 februari 2020, bijlage 25.
[48] Onderzoek ter plaatse van 22 mei 2019, gespreksverslag 4, onder 5 en Onderzoek van 10 februari 2020, bijlage 24.
[49] Onderzoek van 10 februari 2020, bijlage 24.

[VERTROUWELIJK] van OLVG heeft verklaard dat deze twee steekproeven de enige twee steekproeven zijn geweest die OLVG in de periode van 1 januari 2018 tot en met 22 mei 2019 heeft uitgevoerd.[50] Bovendien heeft [VERTROUWELIJK] van OLVG verklaard dat OLVG van mening is dat een verzameling aan incidentele controles ook weer een steekproef vormt, aangezien er geaggregeerd gekeken wordt hoe vaak het voorkomt dat er onrechtmatige inzage geweest is en welke incidenten dit betreft.[51] Volgens de [VERTROUWELIJK] van OLVG zijn daar heel weinig onregelmatigheden in aangetroffen en vormde het niet een specifieke aanleiding om weer een steekproef in te plannen.[52] [VERTROUWELIJK] verklaarde dat er niet, zoals omschreven staat in het loggingbeleid, elke vier weken een steekproefsgewijze controle plaatsvindt maar dat in de praktijk gekeken wordt naar wat aanleiding geeft tot het doen van een steekproef.[53] Bovenvermelde steekproeven zijn de enige twee steekproeven die uitgevoerd zijn.[54] Ten tijde van het onderzoek ter plaatse was een alarmering bij bepaalde grenswaarden nog in ontwikkeling.[55]

Naast deze twee steekproeven heeft OLVG ook incidentele controles gedaan. OLVG heeft in de periode van januari 2018 tot en met april 2019 acht incidentcontroles uitgevoerd.[56] Dit betreft het opvragen van één elektronisch patiëntdossier per keer naar aanleiding van een verzoek van een patiënt.[57]

Naar aanleiding van de zienswijzezitting van 25 juni 2020 heeft OLVG op 13 juli 2020 aanvullende schriftelijke stukken verstrekt, waaronder een data query op alle logging gegevens, rapportages van steekproeven vanuit verschillende perspectieven en rapportages voortvloeiend uit de nieuw gehanteerde selectiemethode.

3.3.3.2 Beoordeling

In paragraaf 3.3.2.2 is reeds uiteengezet dat de verwerkingsverantwoordelijke op grond van artikel 32, eerste lid, van de AVG passende technische en organisatorische maatregelen dient te treffen om een op het risico afgestemd beveiligingsniveau te waarborgen.

De AP heeft vastgesteld dat OLVG in de periode van 1 januari 2018 tot en met 17 april 2019, twee bredere (steekproef) controles van het break-the-glass gedrag uitgevoerd heeft over grotere groepen medewerkers en acht incidentele controles van de logging van één elektronisch patiëntendossier. Voorts heeft de AP vastgesteld dat OLVG in de periode van 1 januari 2018 tot en met 22 mei 2019 geen systematische controles van opvallende afwijkingen van alle logging van alle elektronische patiëntendossiers heeft uitgevoerd, noch systematische of automatische signalering heeft toegepast bij overschrijding van bepaalde grenswaarden in de logging waarbij alle logging van alle elektronische patiëntendossiers betrokken is geweest.

[50] Onderzoek ter plaatse van 22 mei 2019, gespreksverslag 4, onder 5, 10 en 16.
[51] Onderzoek ter plaatse van 22 mei 2019, gespreksverslag 4, onder 8.
[52] Onderzoek ter plaatse van 22 mei 2019, gespreksverslag 4, onder 8.
[53] Onderzoek ter plaatse van 22 mei 2019, gespreksverslag 4, onder 16.
[54] Onderzoek ter plaatse van 22 mei 2019, gespreksverslag 4, onder 16.
[55] Onderzoek ter plaatse van 22 mei 2019, gespreksverslag 4, onder 17.
[56] Onderzoek van 10 februari 2020, bijlagen 16 t/m 23.
[57] Onderzoek van 10 februari 2020, bijlagen 16 t/m 23.

In haar zienswijze geeft OLVG aan dat het protocol "procedure controle op rechtmatigheid dossierinzage" is geactualiseerd en opnieuw vastgesteld op 17 maart 2020. De controle op de logging is sinds het onderzoek ter plaatse van de AP in mei 2019 verder aangescherpt. Per 1 juli 2019 heeft OLVG de frequentie van de controle op de logging reeds opgevoerd naar een keer per twee weken (althans twee of meer rapporten per maand). Deze controle houdt een (tweewekelijkse) data query in op alle logging gegevens. In de periode van juli 2019 tot en met november 2019 zijn er rapportages aan de hand van logging gegevens gemaakt vanuit verschillende perspectieven. Vanuit deze verschillende perspectieven is in deze periode meerdere keren gerapporteerd over het logginggedrag. De verschillende perspectieven zijn mede gebruikt om te kunnen bepalen waar de kans op onrechtmatige inzage het grootst is. Vanaf mei 2020 is er gestart met een nieuwe selectiemethode. Aan alle contacten wordt een score toegekend waarbij een hogere score meer kans betekent op een onrechtmatige inzage. Per juni 2020 wordt er minimaal elke twee weken van een willekeurige dag een uitdraai gemaakt van 50 inzagen met de hoogste puntenscore, welke beoordeeld worden en vervolgens bij verdenking op onrechtmatigheid verder onderzocht worden. Naast de steekproefsgewijze controle vindt ad hoc loggingcontrole plaats indien de actualiteit (vanuit het oplossen van incidenten of vanuit verzoek van een patiënt) hiertoe aanleiding geeft. OLVG is van oordeel dat hiermee voldaan wordt aan norm 12.4.1 van NEN 7510-2 (2017).

Zoals hierboven vermeld heeft de AP vastgesteld dat OLVG in de periode van 1 januari 2018 tot en met 17 april 2019, twee steekproeven en acht incidentele controles van de logging van één elektronisch patiëntendossier heeft uitgevoerd. OLVG heeft daarmee in ieder geval gedurende voornoemde periode niet conform haar eigen beleid (waaronder het Informatiebeveiligings- & privacybeleid en Logging beleid Epic) gehandeld. Afgezien daarvan, is het doen van slechts acht incidentele controles en twee proactieve steekproeven in een periode van 15,5 maanden 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, de gevoelige aard van de gegevens en de risico's voor de persoonlijke levenssfeer van betrokkenen.

OLVG verwerkt op grote schaal (bijzondere categorieën van) persoonsgegevens en (veelal) gaat dit om uiterst gevoelige gegevens over de gezondheid. Er worden derhalve zwaardere eisen gesteld aan de beveiliging van deze gegevens. Gezien de gevoelige aard van de gegevens, de grote omvang van de verwerking en de risico's voor de persoonlijke levenssfeer van betrokkenen had OLVG daarom de loggegevens regelmatig moeten controleren. Op deze manier kan men onbevoegde toegang signaleren en maatregelen nemen. Het uitgangspunt van de AP is dat controle van de logging systematisch en consequent moet plaatsvinden, waarbij een steekproefsgewijze controle en/of controle op basis van klachten niet voldoende is.[58] De fijnmazigheid van het gehanteerde autorisatiemodel en de controle op de juistheid van de autorisaties zijn mede bepalend voor de intensiteit van de controle op de logging. Bij een willekeurig steekproefsgewijs controleren is er geen sprake van een systematiek gericht op onrechtmatig gebruik en risico's. Daarmee heeft OLVG niet aan het vereiste van het regelmatig beoordelen van logbestanden voldaan, wat in de context van deze verwerking in het kader van artikel 32 van de AVG wel is vereist. Een dergelijke controlemaatregel acht de AP, ook gezien de huidige stand van de techniek en de

[58] Zie ook het rapport "Toegang tot digitale patiëntendossiers binnen zorginstellingen" van juni 2013.

uitvoeringskosten, passend. Daarbij neemt de AP in aanmerking dat algemeen geaccepteerde beveiligingsstandaarden, zoals de Nederlandse norm voor informatiebeveiliging in de zorg, regelmatige logging voorschrijven.

Tot slot heeft OLVG, zoals in paragraaf 3.3.2.2. reeds benoemd, zich ook zelfstandig gecommitteerd te voldoen aan NEN-normen. In paragraaf 12.4.1 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.

Gelet op het voorgaande is de AP van oordeel dat OLVG in ieder geval tot 22 mei 2019 artikel 32, eerste lid, van de AVG heeft overtreden doordat OLVG logbestanden niet regelmatig heeft beoordeeld. OLVG heeft inmiddels deze overtreding beëindigd doordat zij de procedure ten aanzien van de controle op de logging aangescherpt heeft en de frequentie van de controle op de logging opgevoerd heeft.

3.4 Overige zienswijze OLVG en reactie AP

3.4.1 Rechten van de verdediging

OLVG stelt dat de oplegging van een boete voor de door de AP geconstateerde gedragingen in strijd is met het nemo-teneturbeginsel[59] zoals neergelegd in artikel 48, eerste lid, van het Europees Handvest en artikel 6, eerste lid, van het Europees Verdrag voor de Rechten voor de Mens (EVRM), aangezien de constateringen gebaseerd zijn op datalekmeldingen die OLVG verplicht was te verrichten onder dreiging van een sanctie. Verwijzend naar verschillende rechtspraak noemt OLVG dat indien gedurende een procedure sprake is van (de redelijke verwachting) van een criminal charge, althans wanneer niet kan worden uitgesloten dat het materiaal tevens in verband met een criminal charge tegen de verstrekker zal worden gebruikt, het nemo-teneturbeginsel eraan in de weg staat dat het in de procedure verkregen wilsafhankelijke materiaal wordt gebruikt voor een bestuursrechtelijke bestraffing door middel van beboeting.[60]

Het feit dat OLVG op grond van het Besluit elektronische gegevensverwerking door zorgaanbieders en de daarin vervatte NEN-normen gehouden is bepaalde logbestanden bij te houden welke het toezicht op de naleving van de AVG mogelijk maakt, maakt volgens OLVG niet dat er sprake is van wilsonafhankelijk bewijsmateriaal. Op grond van artikel 33, eerste lid, van de AVG heeft OLVG op 13 september 2018 en op 15 februari 2019 een melding van een datalek gedaan bij de AP. Deze datalekmeldingen betreffen volgens OLVG informatie die niet los van de wil van OLVG bestaat: OLVG heeft de informatie samengesteld om te voldoen aan de verplichting van artikel 33, eerste lid, van de AVG. Wederom verwijzend naar verschillende rechterlijke uitspraken betoogt OLVG dat wilsafhankelijke informatie niet mag worden gebruikt voor een bestuursrechtelijke bestraffing door middel van beboeting.[61] De AP heeft naar aanleiding van de twee datalekmeldingen een onderzoek ingesteld in het kader waarvan het onderzoek ter plaatste op 22 mei 2019

[59] Het beginsel dat niemand is gehouden tegen zichzelf te getuigen of een bekentenis af te leggen.
[60] Conclusie A-G Vegter 16 mei 2018, ECLI:NL:PHR:2018:441, r.o. 4; CBb 7 mei 2019, ECLI:NL:CBB:2019:177, r.o. 5.3.2; HR 12 juli 2013, ECLI:NL:HR:2013:BZ3640;
[61] HR 12 juli 2013, ECLI:NL:HR:2013:BZ3640, r.o. 3.8 en 3.9.; HR 24 april 2015, ECLI:NL:HR:2015:1117, ECLI:NL:HR2015:1129, ECLI:NL:HR:2015:1130, ECLI:NL:HR2015:1137 en ECLI:NL:HR:2015:1141; CBb 7 mei 2019, ECLI:NL:CBB:2019:177, r.o. 5.3.8 en 5.3.10.

heeft plaatsgevonden. Het is dus volgens OLVG duidelijk dat het gehele onderzoek van de AP gebaseerd is op de door OLVG op grond van de AVG verrichte meldingen.

Bij brief van 17 april 2019 heeft de AP verder op grond van artikel 5:16 en 5:17 van de Algemene wet bestuursrecht (Awb) om informatie verzocht. De AP heeft in deze brief er niet op gewezen dat OLVG niet gehouden is inlichtingen te verstrekken indien zij daarmee bewijzen van een overtreding van de AVG zou leveren. Dat betekent volgens OLVG dat ook alle informatie die de AP heeft verkregen met haar verzoek om inlichtingen, verkregen is onder dwang zoals bedoeld in artikel 6, eerste lid, EVRM en artikel 48, eerste lid, van het Handvest. OLVG concludeert dat gelet op het voorgaande de wilsafhankelijke informatie die onder dwang van OLVG is verkregen niet gebruikt kan worden voor het opleggen van een bestuurlijke boete.

Reactie AP
De AP volgt de zienswijze van OLVG niet. De AP is van oordeel dat het door haar verkregen bewijs niet in strijd met artikel 48, eerste lid, van het Europees Handvest en artikel 6, eerste lid, EVRM en het daarin besloten nemo-teneturbeginsel is verkregen. Evenmin dient bewijs te worden uitgesloten. AP motiveert dat als volgt.

Allereerst zal de AP ingaan op de twee datalekmeldingen. Zoals OLVG zelf aangeeft, zijn de twee gemelde datelekken alleen een aanleiding voor de AP geweest om een ambtshalve onderzoek te starten naar de naleving van artikel 32 van de AVG door OLVG. De twee datalekmeldingen zijn weliswaar in het dossier met de op de zaak betrekking hebbende stukken opgenomen, maar zij vormen op geen enkele wijze bewijs van de door de AP geconstateerde overtreding van artikel 32 van de AVG. Uitsluiting van die datalekmeldingen als bewijs is reeds daarom niet aan de orde. Los daarvan beschouwt de AP de datalekmelding als wilsonafhankelijke informatie. Gelet op artikel 33 lid 5 van de AVG is OLVG gehouden alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen te documenteren, zodat zij geacht wordt over deze gegevens te hebben beschikt.[62]

Ten tweede volgt de AP OLVG niet in haar stelling dat de AP met haar informatieverzoek van 17 april 2019 OLVG heeft gedwongen informatie aan de AP te verstrekken en bijgevolg dat die informatie niet gebruikt mag worden voor het opleggen van een bestuurlijke boete. Daartoe is vooreerst relevant om vast te stellen dat de AP in die brief om informatie heeft verzocht. Er is niet formeel informatie ‘gevorderd’ onder verwijzing naar de medewerkingsplicht, zoals die bijvoorbeeld volgt uit artikel 5:20 van de Awb en/of artikel 31 van de AVG. Dat in de betreffende brief is verwezen naar artikel 58, eerste lid onder a, AVG en artikel 5:16 jo. 5:17 Awb maakt dit niet anders. Die verwijzingen zijn slechts ter informatie voor OLVG in de brief opgenomen teneinde duidelijk te maken dat de AP (en haar medewerkers) OLVG om die informatie mogen verzoeken en op basis waarvan zij dat mogen. Van het verstrekken van informatie onder dwang is naar het oordeel van de AP dan ook geen sprake.

Daar komt bij dat indien en voor zover bewijsuitsluiting (toch) aan de orde zou zijn, die uitsluiting volgens vaste rechtspraak alleen geldt voor bewijsmateriaal waarvan het bestaan afhankelijk is van de wil van de

[62] Zie bijvoorbeeld ook ABRvS 8 april 2020, ECLI:NL:RVS:2020:1011, r.o. 2.2.

verstrekker (wilsafhankelijk materiaal). Dit geldt niet voor bewijsmateriaal dat bestaat onafhankelijk van de wil van de verstrekker (wilsonafhankelijk materiaal). De AP heeft van OLVG in reactie op het informatieverzoek van de AP d.d. 3 mei 2019 zowel wilsafhankelijk materiaal (verklaringen en toelichtingen die voor de AP zijn opgesteld), als wilsonafhankelijk materiaal ontvangen. Het wilsonafhankelijk materiaal bestaat uit documenten die al in fysieke zin bestonden bij OLVG, zoals het loggingbeleid d.d. 29 september 2016 en rapportages van steekproeven d.d. 13 maart 2019 resp. 26 maart 2018. De AP heeft vervolgens het wilsafhankelijke materiaal niet gebruikt voor de vaststelling van de overtreding en de oplegging van de bestuurlijke boete. Wel is de overtreding naast wilsonafhankelijk materiaal, mede gebaseerd op wilsafhankelijk materiaal dat later verstrekt is door medewerkers van OLVG nadat zij door middel van de cautie gewezen zijn op het zwijgrecht. Bewijsuitsluiting is naar het oordeel van de AP dan ook om die reden niet aan de orde.

Op grond van het bovenstaande concludeert de AP de oplegging van een boete voor de geconstateerde gedragingen niet in strijd is met het nemo-teneturbeginsel zoals neergelegd in artikel 48, eerste lid, van het Europees Handvest en artikel 6, eerste lid, EVRM.

3.4.2 Onderzoeksdoel

OLVG betoogt dat de oplegging van een boete voor de door de AP geconstateerde gedragingen, althans die met betrekking tot de authenticatie, in strijd is met de rechten der verdediging zoals neergelegd in artikel 48, tweede lid, van het Europees Handvest en artikel 6, tweede lid, EVRM, aangezien de vastgestelde gedragingen buiten de reikwijdte vallen van het door de AP eerder geformuleerde onderzoeksdoel.

Volgens OLVG concludeert de AP namelijk niet in het onderzoeksrapport dat OLVG geen passende technische en organisatorische maatregelen heeft genomen teneinde te waarborgen dat persoonsgegevens in het elektronische patiëntendossier niet worden geraadpleegd door onbevoegde medewerkers. Maar de AP constateert dat OLVG niet voldoet aan het vereiste van minimaal tweefactor authenticatie ingevolge artikel 32, eerste lid, aanhef, van de AVG. Een tweefactor authenticatie zoals de AP deze invult, voorkomt volgens OLVG de gedragingen van de betrokken medewerkers niet. Bij een tweefactor authenticatie beschikken alle medewerkers, dus ook de werkstudenten, over een pas, token, of een andere tweede factor. Het hebben daarvan betekent niet dat zij niet in staat zouden zijn de gedragingen te verrichten waarop de datalekmeldingen zagen. Deze medewerkers zouden ook met een tweefactor authenticatie zoals de AP die invult de autorisatie hebben gehad die zij thans hebben gehad.

Reactie AP

De AP volgt de zienswijze van OLVG niet. De AP heeft aan OLVG kenbaar gemaakt dat de AP onderzoekt of de technische en organisatorische maatregelen van OLVG ‘passend’ zijn als bedoeld in artikel 32 van de AVG, teneinde te waarborgen dat persoonsgegevens in het elektronische patiëntendossier niet worden geraadpleegd door onbevoegde medewerkers. De AP heeft daarbij expliciet genoemd dat het onderzoek zich hierbij richt op de logische toegangsbeveiliging (authenticatie en autorisatie), logging, controle op de logging en bewustwording van medewerkers.

De conclusie van de AP dat OLVG niet voldoet aan artikel 32, eerste lid, van de AVG nu niet voldaan is aan het vereiste van tweefactor authenticatie houdt direct verband met het onderzoeksdoel en valt binnen de reikwijdte van het onderzoeksdoel. De AP noemt immers artikel 32, eerste lid, van de AVG, de daarbij behorende waarborg en expliciet de logische toegangsbeveiliging (authenticatie en autorisatie) in haar onderzoeksdoel. In het kader van het recht op verdediging is het niet relevant of medewerkers van OLVG met of zonder een tweefactor authenticatie in de praktijk dezelfde autorisatie zouden hebben gehad.

De AP merkt ten overvloede op dat zij in haar onderzoeksdoel het feit dat persoonsgegevens in het elektronische patiëntendossier niet mogen worden geraadpleegd door onbevoegde medewerkers als waarborg heeft genoemd. Om het risico op onbevoegde toegang tot patiëntgegevens te minimaliseren is het van groot belang om vooraf de juiste identiteit van de medewerker vast te stellen. Dat tweefactor authenticatie geen maatregel is die garandeert dat onbevoegde inzage in patiëntendossiers door medewerkers niet meer voorkomt, neemt niet weg dat het een maatregel is die in belangrijke mate bijdraagt aan het voorkomen van onbevoegde toegang en in dit geval vereist is op grond van artikel 32 van de AVG. In dit kader benadrukt de AP dat het toepassen van tweefactor authenticatie en ook de controle op de logging niet op zichzelf staan, maar moeten worden bezien in samenhang met alle andere te nemen passende maatregelen. Het is de combinatie van die maatregelen waardoor OLVG in staat is de bescherming van persoonsgegevens zo goed mogelijk te beheersen en inbreuken zoveel als mogelijk te voorkomen. Het toepassen van een tweefactor authenticatie ontslaat OLVG dan ook niet van de plicht om de bewustwording van medewerkers omtrent de privacybescherming van patiënten te bevorderen.

3.4.3 Invulling artikel 32 van de AVG

OLVG stelt zich op het standpunt dat de AVG lidstaten en derhalve de nationale wetgever geen ruimte biedt om de toetsing aan de norm van artikel 32 van de AVG nader in te vullen door middel van NEN-normen. Volgens OLVG handelt de AP dan ook in strijd met de AVG door dat in het onderzoeksrapport wel te doen. OLVG stelt dat lidstaten uitsluitend dan verder kunnen gaan dan de in de verordening gegeven bescherming, en deze bescherming uitsluitend nader mogen invullen indien dit expliciet in de AVG is bepaald. Hier is volgens OLVG geen sprake van. Volgens OLVG zijn de afwegingen tussen een aantal aspecten zoals opgenomen in artikel 32 van de AVG niet door de AP gemaakt, wat in strijd is met het zorgvuldigheidsbeginsel. Tot slot kunnen de NEN-normen naar het oordeel van OLVG geen basis vormen voor de invulling van artikel 32 van de AVG nu deze normen niet door de AVG genoemd worden en tot stand zijn gekomen zonder gerelateerd te zijn aan of gebaseerd te zijn op de AVG.

Reactie AP

De AP volgt de zienswijze van OLVG ook hierin niet. OLVG wijst op het verbod om nadere (bindende) regels te stellen in nationale regelgeving in het geval er een Europese verordening geldt en deze verordening dit niet expliciet toestaat. Een dergelijke situatie doet zich in casu evenwel niet voor. Naar het oordeel van de AP biedt artikel 6, tweede lid en derde lid, van de AVG daartoe juist uitdrukkelijk wel de mogelijkheid. Dat neemt niet weg dat in het concrete geval artikel 32 van de AVG is toegepast en geïnterpreteerd. De toepassing en interpretatie is - gelet op de haar in artikel 6, derde lid, van de UAVG opgedragen taak om toezicht te houden op de naleving van de AVG - aan de AP. Dat is dan ook wat de AP in het onderzoeksrapport heeft gedaan en waartoe ze gehouden is.

Bij de beantwoording van de vraag of er passende technische en organisatorische maatregelen in de zin van artikel 32 van de AVG zijn is het relevant wat in de betreffende NEN-normen is opgenomen. Deze normen zijn immers algemeen geaccepteerde beveiligingsstandaarden binnen de praktijk van de informatiebeveiliging in de zorg. De in deze NEN-normen vervatte eis van tweefactor authenticatie en de verplichting om de logbestanden regelmatig te beoordelen, acht de AP een concrete invulling van wat als 'passend' kan worden beschouwd in de zin van artikel 32 van de AVG. Dat de NEN-normen niet in de AVG genoemd worden en tot stand zijn gekomen zonder gerelateerd te zijn tot of gebaseerd te zijn op de AVG acht de AP niet relevant. Artikel 32 van de AVG voorziet immers in een norm die zich richt tot alle verwerkingsverantwoordelijken in alle segmenten van de markt. Verwijzend naar paragraaf 3.3.2 en 3.3.3 is door de AP beoordeeld of OLVG voldoende passende beveiligingsmaatregelen heeft getroffen zoals bedoeld in artikel 32 van de AVG, *'rekening houdend met de stand van de techniek en de uitvoeringskosten afgezet tegen de risico's en de aard van de te beschermen persoonsgegevens'*. Bij die afweging heeft de AP de aanwezigheid van algemeen geaccepteerde beveiligingsstandaarden zoals de NEN-normen mede in ogenschouw genomen en mogen nemen.

Bovendien heeft OLVG in haar Informatiebeveiligings- & privacybeleid zelf ook aangegeven dat voornoemd beleid gebaseerd is op de Nederlandse norm voor informatiebeveiliging in de zorg, te weten: NEN 7510, NEN 7512 en NEN 7513 en de actuele wet- en regelgeving, waaronder de AVG.[63] In haar Logging beleid Epic geeft OLVG aan dat dit document moet leiden tot compliance aan NEN7513 en geldende wet- en regelgeving.[64] Kort en goed leidt de AP daaruit af dat ook OLVG van mening is dat deze NEN-normen invulling geven aan de juiste mate van informatiebeveiliging en zich daarom zelfstandig gecommitteerd heeft te voldoen aan bovenstaande NEN-normen.

3.4.4 Besluit elektronische gegevensverwerking door zorgaanbieders

In het onderzoeksrapport van de AP wordt verwezen naar artikel 3, tweede lid, van het Besluit elektronische gegevensverwerking door zorgaanbieders (Begz). Hierin staat vermeld dat een zorgaanbieder overeenkomstig het bepaalde in NEN 7510 en NEN 7512, zorg draagt voor een veilig en zorgvuldig gebruik van het zorginformatiesysteem en een veilig en zorgvuldig gebruik van het elektronisch uitwisselingssysteem waarop hij is aangesloten. OLVG stelt dat de AP alleen een boete of last onder dwangsom kan opleggen ter handhaving van de in de AVG opgelegde verplichtingen en niet voor een overtreding van het Begz. Het Begz is op grond van artikel 26 Wbp vastgesteld en niet op grond van de UAVG. Op grond van artikel 51 UAVG is de Wbp per 25 mei 2018 vervallen. Daarmee is ook de grondslag van het Begz per die datum vervallen.

Reactie AP

De AP volgt de zienswijze van OLVG tot slot ook hierin niet. Zoals in het volgende hoofdstuk wordt uiteengezet, heeft de AP een bestuurlijke boete opgelegd voor de overtreding van artikel 32, eerste lid, van de AVG, meer specifiek ten aanzien van de authenticatie en een regelmatige controle van de logbestanden. Overigens is het Begz wel op het OLVG van toepassing en is zij op grond van het Begz verplicht de normen NEN 7510 en NEN 7512 toe te passen.

[63] Onderzoek van 10 februari 2020, bijlage 2, onder 3.3 en bijlage 8 onder 2.2.
[64] Onderzoek van 10 februari 2020, bijlage 13, onder 2.1.

4. Boete

4.1 Inleiding

OLVG heeft van 25 mei 2018 tot in ieder geval 22 mei 2019 artikel 32, eerste lid, van de AVG overtreden door niet te voldoen aan het vereiste van tweefactor authenticatie en het regelmatig beoordelen van logbestanden.

De AP maakt voor de vastgestelde overtreding gebruik van haar bevoegdheid om aan OLVG een boete op te leggen 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. De AP hanteert hiervoor de Boetebeleidsregels 2019.[65]

Hierna zal de AP eerst kort de boetesystematiek uiteenzetten, gevolgd door de motivering van de boetehoogte in het onderhavige geval.

4.2 Boetebeleidsregels Autoriteit Persoonsgegevens 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 OLVG in geval van een overtreding van artikel 32, eerste lid, van de AVG een bestuurlijke boete op te leggen tot € 10.000.000 of, voor een onderneming, tot 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is.

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

Ingevolge artikel 2, onder 2.1, van de Boetebeleidsregels 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 1 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. […].

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

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.

Ingevolge artikel 7 houdt de AP onverminderd de artikelen 3:4 en 5:46 Awb rekening met de factoren die zijn ontleend aan artikel 83, tweede lid, van de AVG en in de Beleidsregels genoemd onder a tot en met k.

4.3 Boetehoogte

4.3.1. Aard, ernst en duur van de inbreuk

Ingevolge artikel 7, aanhef en 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.

Elke verwerking van persoonsgegevens dient behoorlijk en rechtmatig te geschieden. Persoonsgegevens moeten worden verwerkt op een manier die een passende beveiliging en vertrouwelijkheid van die gegevens waarborgt. Ook ter voorkoming van ongeoorloofde toegang tot of het ongeoorloofde gebruik van persoonsgegevens en de apparatuur die voor de verwerking wordt gebruikt. De verwerkingsverantwoordelijke dient daarom op grond van artikel 32, eerste lid, van de AVG passende en technische en organisatorische maatregelen te treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. Bij het bepalen van het risico voor de betrokkene zijn onder andere de aard van de persoonsgegevens en de aard van de verwerking van belang: deze factoren bepalen de potentiële schade voor de individuele betrokkene bij bijvoorbeeld verlies, wijziging of onrechtmatige verwerking van de gegevens. De AP is tot de conclusie gekomen dat OLVG geen passend beveiligingsniveau heeft gehanteerd voor de verwerking van persoonsgegevens in haar ziekenhuisinformatiesysteem.

De AP heeft vastgesteld dat OLVG tot in ieder geval 22 mei 2019 persoonsgegevens zonder passende beveiliging heeft verwerkt. Deze persoonsgegevens bevatten zeer gevoelige informatie van patiënten van OLVG, zoals een grote verscheidenheid aan gezondheidsgegevens. Daarbij is van belang dat OLVG persoonsgegevens verwerkt van honderdduizenden patiënten. Deze grote groep betrokkenen heeft onnodig extra risico gelopen op onder andere onbevoegde toegang tot hun persoonsgegevens. Het feit dat de overtreding op structurele wijze voor een langere periode heeft voortgeduurd, mede onder de Wbp waaronder ook al een passend beveiligingsniveau was vereist, acht de AP ernstig. Dat het daarnaast een verwerking van bijzonder gevoelige gegevens betreft, maakt een onvoldoende beveiliging van de persoonsgegevens extra kwalijk.

Gelet op de aard, de ernst, de omvang en de duur van de inbreuk ziet de AP aanleiding om het basisbedrag van de boete op grond van artikel 7, aanhef en onder a, van de Boetebeleidsregels te verhogen met €80.000,- tot €390.000,-.

4.3.2 Verwijtbaarheid en nalatige aard van de inbreuk

Ingevolge artikel 5:46, tweede lid, van de Awb houdt de AP bij de oplegging van een bestuurlijke boete rekening met de mate waarin deze aan de overtreder kan worden verweten. Nu het hier gaat om een

overtreding, is voor het opleggen van een bestuurlijke boete conform vaste rechtspraak niet vereist dat wordt aangetoond dat sprake is van opzet en mag de AP verwijtbaarheid veronderstellen als het daderschap vaststaat. Daarnaast houdt de AP op grond van artikel 7, onder b, van de Boetebeleidsregels 2019 rekening met de opzettelijke of nalatige aard van de inbreuk.

OLVG is op grond van artikel 32 van de AVG verplicht om beveiligingsmaatregelen in te voeren die passend zijn voor de aard en omvang van de verwerkingen die OLVG uitvoert. Nu OLVG voor langere periode geen tweefactor authenticatie en het regelmatig controleren van de logbestanden in haar organisatie heeft geïmplementeerd, is de AP van oordeel dat OLVG in elk geval bijzonder nalatig is geweest in het niet treffen van dergelijke maatregelen. Van OLVG mag mede gelet op de gevoelige aard en de grote omvang van de verwerking wel worden verwacht dat zij zich van de voor haar geldende normen vergewist en daar naar handelt. De AP acht dit verwijtbaar.

Daarnaast heeft OLVG in haar eigen Informatiebeveiligings- & privacybeleid aangegeven dat voornoemd beleid is gebaseerd op de Nederlandse norm voor informatiebeveiliging in de zorg, te weten: NEN 7510, NEN 7512 en NEN 7513 en de actuele wet- en regelgeving, waaronder de AVG. OLVG streeft daarbij aantoonbaar te voldoen aan deze normen. OLVG heeft verder in haar loggingbeleid bepaald dat zij voor de controle van de loggegevens elke vier weken een representatieve steekproef neemt om te analyseren. Het feit dat OLVG dus ook niet voldoet aan haar eigen bestaande beleidsregels acht de AP zeer nalatig. Het had op de weg van OLVG gelegen om de normen te implementeren en de overtreding van artikel 32 van de AVG zo spoedig mogelijk te beëindigen, zodat onder andere het signaleren van onbevoegde toegang tot patiëntgegevens en het treffen van maatregelen naar aanleiding van onbevoegde toegang gewaarborgd is.

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 €50.000,- tot €440.000.

4.3.3 Evenredigheid

Tot slot beoordeelt de AP ingevolge artikelen 3:4 en 5:46 van de Awb 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. De AP is van oordeel dat, gezien de ernst van de overtreding en de mate waarin deze aan OLVG kan worden verweten, de (hoogte van) de boete evenredig is.[66] De AP ziet geen aanleiding het bedrag van de boete op grond van de evenredigheid en de overige in artikel 7 van de Boetebeleidsregels genoemde omstandigheden, voor zover van toepassing in het voorliggende geval, te verhogen of te verlagen.

4.4 Conclusie

De AP stelt het totale boetebedrag vast op €440.000,-.

[66] Zie hiervoor paragraaf 4.3.1 en 4.3.2.

Datum
26 november 2020

Ons kenmerk
[VERTROUWELIJK]

5. Dictum

Boete

De AP legt aan OLVG, wegens overtreding van artikel 32, eerste lid, van de AVG een bestuurlijke boete op ten bedrage van **€ 440.000,--** (zegge vierhonderdenveertigduizend euro).[67]

Hoogachtend,
Autoriteit Persoonsgegevens,

w.g.

drs. C.E. Mur
Bestuurslid

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. Het indienen van een bezwaarschrift schort de werking van dit besluit op. 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.

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