ECLI:NL:RBDHA:2021:3090

Instantie	Rechtbank Den Haag
Datum uitspraak	31-03-2021
Datum publicatie	15-04-2021
Zaaknummer	AWB - 20 _ 1516
Rechtsgebieden	Bestuursrecht
Bijzondere kenmerken	Eerste aanleg - meervoudig
Inhoudsindicatie	Boete (€ 460.000,-) en last onder dwangsom op grond van de Algemene Verordening gegevensbescherming (AVG). Overtreding artikel 32 van de AVG. De rechtbank ziet aanleiding de boete te matigen tot € 350.000,-..
Vindplaatsen	Rechtspraak.nl

Uitspraak

RECHTBANK DEN HAAG

Bestuursrecht

zaaknummer: SGR 20/1516

uitspraak van de meervoudige kamer van 31 maart 2021 in de zaak tussen

Stichting [eiseres] , te [vestigingsplaats] , eiseres

(gemachtigden: mr. W.R. Kastelein, mr. A.C. Beijering-Beck en mr. R. Ketting),

en

de Autoriteit Persoonsgegevens, verweerder

(gemachtigden: mr. E. Nijhof en mr. J.M.A. Koster).

Procesverloop

Bij besluit van 18 juni 2019 (het primaire besluit) heeft verweerder aan eiseres een boete en een last onder dwangsom opgelegd.

Bij besluit van 15 januari 2020 (het bestreden besluit) heeft verweerder het bezwaar van eiseres ongegrond verklaard.

Eiseres heeft tegen het bestreden besluit beroep ingesteld.

Verweerder heeft een verweerschrift ingediend.

Het onderzoek ter zitting heeft plaatsgevonden op 3 februari 2021.

Namens eiseres zijn verschenen [A] (voorzitter Raad van Bestuur) en [B] (jurist van de Raad van Bestuur) en de gemachtigden mr. W.R. Kastelein en

mr. A.C. Beijering-Beck.

Verweerder heeft zich laten vertegenwoordigen door zijn gemachtigden.

Overwegingen

1. De relevante wet- en regelgeving is opgenomen in de bijlage bij deze uitspraak. Deze bijlage is onderdeel van de uitspraak.

2. Op 4 april 2018 heeft eiseres een melding gedaan van een datalek aan verweerder. Het datalek had betrekking op onrechtmatige inzage in een patiëntendossier van een bekende Nederlander. Naar aanleiding van die melding heeft verweerder bij brief van 23 april 2018 een schriftelijk informatieverzoek verstuurd aan eiseres. Verweerder heeft naar aanleiding van de door eiseres toegezonden informatie met toepassing van artikel 58, eerste lid, aanhef en onder b, van de Algemene Verordening Gegevensbescherming (AVG) besloten nader onderzoek te doen naar, voor zover hier van belang, de toegang tot patiëntgegevens in de digitale patiëntendossiers bij eiseres. De resultaten van het nader onderzoek zijn vastgelegd in het onderzoeksrapport “Toegang tot digitale patiëntdossiers door medewerkers van het [eiseres] , Voorlopige bevindingen” van januari 2019. Verweerder heeft geconcludeerd dat eiseres (vanaf januari 2018) onvoldoende passende maatregelen heeft genomen als bedoeld in artikel 32, eerste lid, van de AVG. In de eerste plaats heeft verweerder aan eiseres tegengeworpen dat geen sprake was van tweefactor authenticatie. Het was voor gebruikers van het ziekenhuisinformatiesysteem mogelijk om toegang krijgen tot de gegevens in de digitale patiëntendossiers met alleen iets wat een gebruiker weet (namelijk een gebruikersnaam en wachtwoord). In dat geval wordt gebruik gemaakt van éénfactor authenticatie. Het ziekenhuisinformatiesysteem van eiseres had niet de ingebouwde verplichting, maar alleen de mogelijkheid om met tweefactor authenticatie in te loggen. Verder heeft verweerder aan de besluiten ten grondslag gelegd dat eiseres de logging van de toegang tot de patiëntendossiers niet regelmatig gecontroleerd heeft. Logging houdt in dat een zorginstelling structureel bijhoudt wie wanneer welk patiëntendossier heeft geraadpleegd zodat onbevoegde toegang kan worden gedetecteerd en zo nodig maatregelen genomen kunnen worden. Het beleid van eiseres voorzag in een aselecte steekproef van jaarlijks zes patiëntdossiers. In de relevante periode waarop het onderzoek van verweerder zag is er proactief één controle op ongeautoriseerde inzage geweest en zes controles op verzoek van patiënten en medewerkers. Eén controle in de periode van januari 2018 tot en met oktober 2018 kan, afgezet tegen het aantal patiëntbezoeken dat eiseres jaarlijks krijgt (in 2017 afgerond 381.500) en het aantal medewerkers dat (potentieel) toegang tot de patiëntendossiers heeft, volgens verweerder niet worden beschouwd als regelmatige controle. De in die periode door eiseres uitgevoerde reactieve controles kunnen evenmin worden beschouwd als

regelmatige controle. Ook de zes (proactieve) controles op de logging die eiseres heeft aangekondigd en uitgevoerd in 2019 acht verweerder, wederom afgezet tegen het aantal patiëntbezoeken en het aantal medewerkers, onvoldoende om als regelmatig te kunnen worden aangemerkt.

Verweerder heeft daarom aan eiseres een bestuurlijke boete opgelegd. De hoogte van de bestuurlijke boete is vastgesteld op € 460.000,-. Hierbij heeft verweerder zich gebaseerd op de Boetebeleidsregels Autoriteit Persoonsgegevens 2019 (Boetebeleidsregels 2019). Ook is een last onder dwangsom opgelegd vanwege dezelfde overtreding. De last strekt ertoe dat eiseres de toegang tot haar ziekenhuisinformatiesysteem uitsluitend mogelijk maakt met toepassing van tweefactor authenticatie, en dat de logbestanden regelmatig worden gecontroleerd op onrechtmatige toegang of onrechtmatig gebruik van patiëntgegevens. De begunstigingstermijn is 15 weken. De hoogte van de dwangsom is door verweerder vastgesteld op € 100.000,- voor iedere twee weken na afloop van de begunstigingstermijn, tot een maximumbedrag van in totaal € 300.000,-. Verweerder heeft de boete en de last onder dwangsom in bezwaar gehandhaafd.

Het nemo tenetur-beginsel

3. Eiseres voert aan dat sprake is van strijd met het nemo tenetur-beginsel.

Op grond van vaste rechtspraak geldt 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 tenetur-beginsel eraan in de weg staat dat het in de procedure verkregen wilsafhankelijke materiaal wordt gebruikt voor een bestuursrechtelijke bestraffing door middel van beboeting. Eiseres heeft hierbij verwezen naar de uitspraak van de Hoge Raad van 12 juli 2013, ECLI:NL:HR:2013:BZ3640. De datalekmelding en de informatie in de datalekmelding betreffen informatie die niet los van de wil van eiseres bestaat. Eiseres heeft het materiaal samengesteld om te voldoen aan de verplichting van artikel 33, eerste lid, van de AVG. Het hele onderzoek van verweerder is gebaseerd op de door eiseres op grond van de AVG gedane melding. Ondanks vermelding van de zinsnede dat eiseres niet verplicht is te antwoorden op vragen waarmee zij zichzelf kan belasten, is haar feitelijk geen keus gelaten. Ook is deze formulering zodanig algemeen en vaag dat niet duidelijk is dat daarmee op een boete wordt gedoeld. Dat betekent dat ook de informatie die verweerder heeft verkregen met haar verzoek om inlichtingen van 12 oktober 2018 is verkregen onder dwang.

4. Er bestaat geen grond voor het oordeel dat de door verweerder verkregen informatie niet ten grondslag mocht worden gelegd aan de boete vanwege schending van het nemo tenetur-beginsel. Dit beginsel, dat onder meer besloten ligt in artikel 6 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM), houdt in dat niemand is gehouden tegen zichzelf te getuigen of een bekentenis af te leggen. De rechtbank stelt vast dat verweerder de boete en de last onder dwangsom niet heeft gebaseerd op de informatie in de datalekmelding. Wel heeft verweerder naar aanleiding van de datalekmelding bij brief van 23 april 2018 informatie opgevraagd bij eiseres over de resultaten van het interne onderzoek en de al dan niet getroffen verbetermaatregelen. Verweerder heeft terecht gesteld dat de rapportage van het interne onderzoek dat eiseres heeft ingediend, wilsonafhankelijk materiaal betreft. Het gaat om een onderzoek dat reeds vóór de datalekmelding en het verzoek om de rapportage was gestart. Ook het overzicht van getroffen maatregelen in dit onderzoek betreft naar het oordeel van de rechtbank wilsonafhankelijk materiaal. Zoals verweerder stelt, vergde het schriftelijke inlichtingenverzoek van 23 april 2018 niet van eiseres alsnog bewijs te verzamelen, maar slechts om de resultaten van het gedane onderzoek beschikbaar te stellen aan verweerder. Er is dan ook sprake van een andere situatie dan in de door eiseres genoemde uitspraak. Bestaand wilsonafhankelijk materiaal dat beschikbaar is gesteld ter naleving van een inlichtingenvordering, levert volgens vaste rechtspraak geen schending van artikel 6 van het EVRM op (zie bijvoorbeeld de uitspraak van het College van Beroep voor het bedrijfsleven, 4 september 2018, ECLI:NL:CBB:2018:444). In de ontvangen informatie heeft verweerder vervolgens aanleiding gezien een onderzoek te starten naar de naleving van artikel 32 van de AVG. In dat kader is op 12 oktober 2018 een inlichtingenverzoek gedaan, waarbij is verzocht om documenten en vragen zijn gesteld. Naar het oordeel van de rechtbank is eiseres

met het gebruik van het woord “cautie” in combinatie met de zinsnede “u bent niet verplicht te antwoorden op vragen waarmee u uzelf of uw organisatie kunt belasten” in de brief van 12 oktober 2018 voldoende duidelijk gewezen op haar zwijgrecht.

De rechten van verdediging

5. Eiseres voert verder aan dat verweerder de rechten van verdediging, neergelegd in artikel 6, tweede lid, van het EVRM en 48, tweede lid, van het Handvest van de grondrechten van de EU heeft geschonden, omdat verweerder het onderzoek heeft uitgebreid ten opzichte van de onderzoeksopdracht waarvan zij eiseres op de hoogte heeft gesteld. Eiseres heeft verwezen naar het arrest Dow Benelux/Commissie (zaak 85/87) en het arrest Deutsche Bahn AG/Commissie (C-583/13P). Het onderzoek had uitdrukkelijk betrekking op de raadpleging door onbevoegde medewerkers. In het onderzoeksrapport heeft verweerder dit uitgebreid tot de verwerking van patiëntengegevens in het ziekenhuisinformatiesysteem van eiseres. De constatering van verweerder dat eiseres niet heeft voldaan aan het vereiste van tweefactor authenticatie heeft geen betrekking op een onderzoek dat binnen de reikwijdte van het door hem geformuleerde onderzoeksdoel valt.

6. Er bestaat geen grond voor het oordeel dat verweerder de rechten van verdediging heeft geschonden en daarom de boete niet mocht opleggen op basis van het onderzoek. De rechtbank stelt vast dat aan eiseres in de brief van 12 oktober 2018 kenbaar is gemaakt dat verweerder onderzoekt of de technische en organisatorische maatregelen die zijn getroffen teneinde te waarborgen dat persoonsgegevens in het digitale patiëntendossier niet worden ingezien door onbevoegde medewerkers passend zijn als bedoeld in artikel 32 van de AVG. In de bijlage bij deze brief zijn vragen gesteld over de toegangsbeveiliging, de logging en het melden van een inbreuk in verband met persoonsgegevens (datalek). Verweerder stelt naar het oordeel van de rechtbank terecht dat authenticatie, de techniek waarmee een systeem kan vaststellen wie een gebruiker is, onderdeel uitmaakt van de toegangsbeveiliging. De stelling van eiseres dat een tweefactor authenticatie niet zou voorkomen dat geautoriseerde, maar onbevoegde medewerkers de gegevens inzien doet hier niet aan af. Het enkele feit dat niet in elk stuk exact dezelfde bewoordingen worden gebruikt, betekent ten slotte niet dat het onderzoek reeds daarmee een andere reikwijdte heeft gekregen, laat staan dat daarmee het verdedigingsbelang van eiseres is geschaad.

De grondslag van de boete en de last onder dwangsom

7. Eiseres voert vervolgens aan dat verweerder de boete en de last onder dwangsom heeft gebaseerd op het Besluit elektronische gegevensverwerking door zorgaanbieders (Begz) en de NEN-normen 7510 en 7513. Het gebruik van de woorden “in samenhang met” in het boetebesluit duidt erop dat alle genoemde artikelen gezamenlijk ten grondslag zijn gelegd aan de besluiten. Dit volgt ook uit de wijze waarop verweerder het wettelijk kader heeft geschetst, waarbij de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg en de het Begz zijn genoemd. Verweerder heeft ten onrechte rechtstreeks aan deze bepalingen getoetst. Verweerder heeft daarmee artikel 32 van de AVG onjuist toegepast. Door de NEN-normen toe te passen is geen sprake meer van een toepassing of interpretatie. Artikel 32 van de AVG benoemt een aantal aspecten waarbij een afweging moet worden gemaakt. Verweerder heeft dit op geen enkele manier gedaan, omdat zij geen interpretatie van artikel 32 van de AVG heeft gegeven, maar een NEN-norm direct heeft toegepast. De NEN-normen zijn niet gerelateerd aan of gebaseerd op de AVG. Er is dan ook sprake van strijd met het zorgvuldigheidsbeginsel en het motiveringsbeginsel.

8. De rechtbank stelt vast dat de boete en de last onder dwangsom zijn gebaseerd op het niet nemen van passende technische en organisatorische maatregelen in de zin van artikel 32, eerste lid, van de AVG. Dat in het primaire besluit staat dat artikel 32 van de AVG in samenhang moet worden gelezen met artikel 3, tweede lid, van het Begz en het bepaalde onder 9.4.1 van NEN 7510-2, betekent niet dat de Begz of de NEN-normen ook rechtstreeks aan de handhaving ten grondslag zijn gelegd. Verweerder heeft gesteld dat hij artikel 32 van de AVG moet interpreteren en dat de in de NEN-normen vervatte eis van tweefactor authenticatie en de eis om logbestanden regelmatig te

beoordelen, de concrete invulling vormen van wat in dit geval als ‘passend’ kan worden beschouwd. Verweerder heeft ter zitting toegelicht dat een concrete invulling met andere maatregelen mogelijk is als dit voldoende wordt gemotiveerd en deze maatregelen afdoende zijn.

9. De rechtbank stelt voorop dat verweerder op grond van artikel 6, tweede lid, van de Uitvoeringswet Algemene verordening gegevensbescherming bevoegd is om een nadere uitwerking van en invulling te geven aan artikel 32 van de AVG. De rechtbank is verder van oordeel dat verweerder eiseres mocht tegenwerpen dat zij zich niet aan de NEN-normen heeft gehouden. Hierbij wordt in aanmerking genomen dat eiseres in haar eigen informatiebeveiligingsbeleid zelf heeft gekozen voor een invulling van passende technische en organisatorische maatregelen door middel van toepassing van de NEN-normen. De NEN-normen zijn algemeen geaccepteerde beveiligingsstandaarden binnen de praktijk van de informatiebeveiliging in de zorg, zoals ook blijkt uit de vastlegging daarvan in de Begz. Daarbij komt dat de eis van tweefactor authenticatie en de eis van de controle op de logging ook onder het oude regime van de Wet bescherming persoonsgegevens (Wbp) werden gezien als passende maatregelen, hetgeen ook aan eiseres bekend kon zijn. Bovendien is niet gebleken van andere maatregelen die eiseres zou hebben getroffen die de tweefactor authenticatie en regelmatige controle op de logging overbodig zouden maken.

Het legaliteitsbeginsel

10. Eiseres voert verder aan dat artikel 32, eerste lid, van de AVG een open norm is die is nog niet is ingevuld. Het is in strijd met het legaliteitsbeginsel om handhavend op te treden wegens een vermeend handelen in strijd met een norm waarvan de strekking en reikwijdte (nog) niet duidelijk zijn. Bovendien is ook het “regelmatig beoordelen van logbestanden” een open norm.

11. Volgens vaste jurisprudentie van de Afdeling (zie bijvoorbeeld de uitspraak van 17 april 2019, ECLI:NL:RVS:2019:1235) verlangt het lex certa-beginsel, dat onder meer besloten ligt in artikel 7 van het EVRM, van de wetgever dat hij met het oog op de rechtszekerheid op een zo duidelijk mogelijke wijze de verboden gedragingen omschrijft. Daarbij moet niet uit het oog worden verloren dat de wetgever soms met een zekere vaagheid, bestaande uit het gebruik van algemene termen, verboden gedragingen omschrijft om te voorkomen dat gedragingen die strafwaardig zijn buiten het bereik van die omschrijving vallen. Die vaagheid kan onvermijdelijk zijn, omdat niet altijd te voorzien is op welke wijze de te beschermen belangen in de toekomst zullen worden geschonden en omdat, indien dit wel is te voorzien, de omschrijvingen van verboden gedragingen anders te verfijnd worden met als gevolg dat de overzichtelijkheid wegvalt en daarmee het belang van de algemene duidelijkheid van wetgeving schade lijdt.

12. De rechtbank is van oordeel dat geen sprake is van strijd met het legaliteitsbeginsel. Hiertoe wordt overwogen dat de AVG niet alleen van toepassing is in de zorg en dat de tekst dus voldoende algemeen moet zijn om voor alle verwerkingsverantwoordelijken en verwerkers te kunnen gebruiken. Verder stond het begrip ‘passende technische en organisatorische maatregelen’ ook in de Wbp, die eveneens was gebaseerd op Europese regelgeving, namelijk Richtlijn 95/46/EG. Naar het oordeel van de rechtbank heeft verweerder daarnaast terecht gesteld dat geen sprake is van een volledig open norm, omdat de norm nader wordt geconcretiseerd in het eerste lid ten aanzien van de passende maatregelen en in het tweede lid waar de verwerkingsrisico’s worden genoemd. Verder leidt de omstandigheid dat verweerder niet op voorhand kan aangeven wanneer sprake is van regelmatige controle van de logbestanden, naar het oordeel van de rechtbank niet tot de conclusie dat sprake is van een dermate open norm dat sprake is van strijd met het legaliteitsbeginsel. De norm is naar het oordeel van de rechtbank voldoende duidelijk. Hierbij wordt in aanmerking genomen dat eiseres zich, zoals verweerder stelt, als professionele partij kan vergewissen van de juiste toepassing van de normen. In elk geval kon voor eiseres duidelijk zijn dat het in haar beleid opgenomen aantal van zes controles niet voldeed aan de norm, gelet op het aantal patiëntbezoeken en het aantal medewerkers. Er bestaat dan ook geen grond voor het oordeel dat verweerder de norm had moeten verduidelijken voordat tot handhaving werd overgegaan. Ter zitting heeft eiseres er in dit verband op gewezen dat het de taak van verweerder is te bevorderen dat gedragscodes worden opgesteld die bijdragen tot de juiste

toepassing van de AVG, maar dat het de ziekenhuizen zelf zijn die het initiatief hebben genomen om een gedragscode op te stellen. Verweerder heeft echter terecht gesteld dat de gedragscode een instrument van de sector zelf is en niet van verweerder. Verweerder kan een voorgelegde gedragscode alleen goedkeuren. Of er een gedragscode is opgesteld, is dan ook niet bepalend voor de vraag of verweerder handhavend mocht optreden.

13. De rechtbank overweegt dat verweerder gelet op het voorgaande in beginsel bevoegd was om handhavend op te treden.

Het gelijkheidsbeginsel

14. Eiseres voert aan dat sprake is van strijd met het gelijkheidsbeginsel, omdat verweerder in andere zaken een andere uitleg heeft gegeven aan artikel 32 van de AVG en zowel ten aanzien van de tweefactor authenticatie als de controle op de logging ten nadele van haar is afgeweken van de gedragslijn. Eiseres heeft verwezen naar besluiten met betrekking tot twee zorgverzekeraars over logging en een besluit van het UWV over tweefactor authenticatie. Ten aanzien van de twee zorgverzekeraars achtte verweerder een reactieve controle van de logbestanden voldoende en is een lagere sanctie opgelegd terwijl de omvang van de overtreding juist groter was. Het UWV paste éénfactor authenticatie toe. In deze zaken is alleen een last onder dwangsom opgelegd, terwijl aan eisers een boete en een last onder dwangsom zijn opgelegd.

15. Naar het oordeel van de rechtbank is geen sprake van een ongelijke behandeling van gelijke gevallen. Verweerder stelt terecht dat uit de last onder dwangsom die aan de twee zorgverzekeraars is opgelegd, niet blijkt dat verweerder in die gevallen een reactieve controle voldoende achtte. In de last staat dat er “in ieder geval” een reactieve controle mogelijk moet zijn. Verweerder heeft toegelicht dat sprake was van een onderzoek dat door de rechtbank in een tussenuitspraak precies was omschreven en dat verweerder zich vanwege de beschikbare tijd hieraan gehouden heeft. Er is daarom, anders dan in het geval van eiseres, geen specifiek onderzoek gedaan naar de beveiligingsmaatregelen. Verder heeft verweerder er terecht op gewezen dat het onderzoek is uitgevoerd onder de Wbp, waarbij als vaste gedragslijn gold dat het opleggen van een boete als ultimum remedium gold. Ook de situatie van het UWV betreft geen gelijk geval. Bij het UWV ging het om een werkgeversportaal, een overheidsdienst waar externen toegang tot dienen te krijgen. In het geval van eiseres gaat het om toegang van de eigen medewerkers tot het zorginformatiesysteem. Ook in het geval van het UWV geldt dat het onderzoek was afgerond vóór de inwerkingtreding van de AVG. Verweerder heeft toegelicht dat het UWV een langere begunstigingstermijn heeft gekregen voor het invoeren van de tweefactor authenticatie omdat sprake was van andere omstandigheden. Verweerder heeft ter zitting gesteld dat bij het bepalen van de begunstigingstermijn rekening is gehouden met de tijd die eiseres zelf stelde nodig te hebben om de tweefactor authenticatie, waar zij al over beschikte, verplicht te maken.

De hoogte van de boete; evenredigheid

16. Eiseres voert aan dat de hoogte van de opgelegde boete strijdig is met het evenredigheidsbeginsel en het zorgvuldigheidsbeginsel. In het onderzoeksrapport komt verweerder tot de conclusie dat de beveiligingsmaatregelen die eiseres heeft getroffen grotendeels volstonden. De conclusie van verweerder dat eiseres “bijzonder nalatig” is geweest is dan ook ongegrond en niet terug te voeren op de onderzoeksbevindingen. Verder is de opgelegde basisboete van € 310.000,- bijzonder hoog vergeleken met boetes die in het buitenland zijn opgelegd. Ten onrechte is de boete verhoogd vanwege de “aard, ernst en duur van de inbreuk” en “de nalatige aard”. Ook komt de onderbouwing van de eerste verhoging op hetzelfde neer als de onderbouwing van de tweede verhoging. Verweerder heeft de boete ten onrechte niet verlaagd wegens schadebeperkende maatregelen als bedoeld in artikel 7, aanhef en onder c, van de Boetebeleidsregels 2019. Ook had de boete moeten worden verlaagd vanwege de financiële draagkracht van eiseres.

17. Volgens vaste jurisprudentie van de Afdeling (vergelijk de uitspraak van 27 januari 2021, ECLI:NL:RVS:2021:170) moet een bestuursorgaan bij het toepassen van de bevoegdheid om een boete op te leggen de hoogte van de boete afstemmen op de ernst van de overtreding en de mate waarin deze aan de overtreder kan worden verweten. Daarbij moet rekening worden gehouden met de omstandigheden waaronder de overtreding is gepleegd. Dit is geregeld in artikel 5:46, tweede lid, van de Awb. Verweerder heeft beleidsregels vastgesteld waarin de boetebedragen voor de overtredingen zijn vastgesteld. Ook als de rechter het beleid niet onredelijk heeft bevonden, moet verweerder bij de toepassing daarvan in een individueel geval beoordelen of die toepassing in overeenstemming is met de hiervoor bedoelde wettelijke eisen aan de uitoefening van de boetebevoegdheid. Steeds moet de boete, zo nodig in aanvulling op of in afwijking van het beleid, zo worden vastgesteld dat deze evenredig is. De rechter toetst het besluit van het bestuursorgaan zonder terughoudendheid.

18. Uit artikel 2.3 van de van de Boetebeleidsregels 2019 volgt dat voor overtreding van artikel 32 van de AVG een basisboetebedrag van € 310.000,- geldt. Op grond van de factoren genoemd in artikel 7 van de Boetebeleidsregels 2019 kan de basisboete worden verhoogd of verlaagd. Verweerder heeft de boete tweemaal verhoogd met € 75.000,- vanwege de factoren uit artikel 7, aanhef en onder a (aard, ernst en duur van de inbreuk) en b (opzettelijke/nalatige aard van de inbreuk).

19. Verweerder heeft naar het oordeel van de rechtbank terecht gesteld dat alleen aan de hand van de basisboete, die nog niet is afgestemd op de diverse factoren, geen vergelijking kan worden gemaakt met vergelijkbare gevallen in andere landen. Verder stelt de rechtbank vast dat eiseres niets heeft ingebracht tegen de hoogte van de basisboete als beleidsmatig uitgangspunt. De rechtbank is dan ook van oordeel dat een basisboetebedrag van € 310.000,- niet onredelijk is. Verweerder heeft naar het oordeel van de rechtbank terecht gesteld dat de boeteverhogende factor “aard, ernst en duur van de inbreuk” zich heeft voorgedaan, gelet op de omstandigheid dat sinds januari 2018 tot en met 18 juni 2019 geen passende beveiligingsmaatregelen zijn getroffen, omdat sprake is van een groot aantal patiënten dat is opgenomen in het ziekenhuisinformatiesysteem en gelet op het type persoonsgegevens dat bijzondere bescherming behoeft. Ook de boeteverhogende factor “nalatige aard” heeft zich naar het oordeel van de rechtbank voorgedaan. Hiertoe wordt overwogen dat eiseres niet de juiste maatregelen heeft getroffen nadat het datalek zich heeft voorgedaan. Dit klemt temeer nu eiseres heeft aangevoerd voorafgaand aan het datalek in 2018 simpelweg geen tijd te hebben gehad voor regelmatige controle van de logbestanden. Verweerder heeft terecht gesteld dat eiseres eerder initiatief had moeten tonen. De rechtbank volgt de stelling van eiseres dat de onderbouwing van de eerste verhoging op hetzelfde neerkomt als de onderbouwing van de tweede verhoging dan ook niet. Verder heeft verweerder zich terecht op het standpunt gesteld dat aan de boetebepalende factor zoals vermeld in artikel 7, aanhef en onder c, van de Boetebeleidsregels 2019, niet is voldaan, nu geen sprake is van maatregelen die de door betrokkenen geleden schade beperken.

20. Gelet op het voorgaande mocht verweerder de basisboete op grond van het beleid verhogen. De rechtbank is echter van oordeel dat de verhoging met tweemaal € 75.000,- bovenop de basisboete in dit geval tot een boetebedrag leidt dat niet evenredig is. Hierbij wordt in aanmerking genomen dat eiseres ten tijde van belang wel maatregelen heeft genomen om te voorkomen dat persoonsgegevens in het digitale patiëntendossier worden ingezien door onbevoegde medewerkers, zoals onder meer de invoering van een extra waarschuwing die in beeld komt als een medewerker een dossier opent, de verplichtstelling van een e-learningcursus voor alle medewerkers die toegang hebben tot het elektronische patiëntendossier, de aanscherping van de arbeidsovereenkomsten en het waar mogelijk aanscherpen van autorisaties. Dat eiseres, zoals verweerder stelt, wettelijk verplicht was deze maatregelen te nemen, maakt niet dat de invoering daarvan geen enkele rol kan spelen in het kader van de evenredigheid. Artikel 7, aanhef en onder d, van de Boetebeleidsregels 2019 maakt het immers expliciet mogelijk rekening te houden met andere maatregelen die in dit kader zijn getroffen. Daarbij komt dat eiseres nog tijdens de bezwaarfase maatregelen heeft getroffen om te voldoen aan artikel 32 van de AVG, door tweefactor authenticatie in te voeren en de logging te intensiveren. Al deze door eiseres getroffen maatregelen tonen in ieder geval de bereidwilligheid van eiseres om met de problematiek in de organisatie aan de slag te gaan en nuanceren de nalatigheid die eiseres wordt verweten. Verweerder heeft hier ten onrechte geen gewicht aan toegekend. De rechtbank ziet daarom aanleiding om het boetebedrag te matigen tot een bedrag van € 350.000,-.

21. Er bestaat geen grond voor het oordeel dat de boete verder gematigd zou moeten worden vanwege de financiële draagkracht van eiseres. De rechtbank neemt hierbij in aanmerking dat het bedrijfsresultaat in 2019 € 1.813.746,- was en eiseres de beschikking had over € 30.598.630,- aan vrij beschikbare liquide middelen. De omstandigheden als gevolg van de Coronacrisis leiden niet tot een ander oordeel, nu eiseres niet heeft betwist dat door de zorgverzekeraars de effecten van corona op de zorgomzet van ziekenhuizen wordt geneutraliseerd en de netto extra kosten gemaakt vanwege corona, worden vergoed.

22. De rechtbank is concluderend van oordeel dat de opgelegde boete in dit geval leidt tot een onevenredige sanctie en dat matiging van de boete tot een bedrag van € 350.000,- passend en geboden is. Verweerder heeft de boete ten onrechte niet gematigd.

De last onder dwangsom

23. Eiseres voert aan dat de last onvoldoende nauwkeurig is omschreven. Uit de last blijkt niet dat het controleproces dynamisch en aan verandering onderhevig is. Dit heeft verweerder echter wel gesteld in de brief van 2 december 2019, waarin is vastgesteld dat eiseres op dat moment aan de last voldeed. Ook is de last onder dwangsom in strijd met het evenredigheidsbeginsel, omdat de hoogte is gerelateerd aan het datalek en de last ten onrechte niet is gesplitst naar aanleiding van de twee van elkaar onafhankelijke maatregelen die eiseres moest nemen. Verder is de last onder dwangsom in strijd met het gelijkheidsbeginsel, omdat in andere (ernstigere) gevallen lagere dwangsommen zijn vastgesteld.

24. Er bestaat geen grond voor dat de last onvoldoende nauwkeurig is omschreven. Verweerder stelt naar het oordeel van de rechtbank terecht dat de last twee maatregelen betreft die allebei verband houden met de naleving van artikel 32 van de AVG. Als één van de maatregelen wel wordt uitgevoerd en de andere niet, leidt dat nog altijd tot de conclusie dat onvoldoende passende beveiligingsmaatregelen zijn getroffen. Verweerder heeft dan ook geen aanleiding hoeven zien om de verschillende onderdelen te splitsen. Verder stelt verweerder terecht dat uit artikel 32 van de AVG reeds voortvloeit dat de verplichting om passende maatregelen te treffen dynamisch van aard is. Verweerder heeft toegelicht dat hij in de brief van 2 december 2019 duidelijk heeft willen maken dat de wijze waarop de controle van de logbestanden plaats dient te vinden, als uitvloeisel van artikel 32 van de AVG, dynamisch van aard is en dat dit verband houdt met het tijdgebonden karakter van de stand van de techniek en de mogelijkheid om tijdig te kunnen inspelen op eventuele veranderde omstandigheden en toekomstige ontwikkelingen. Hiermee is geen afbreuk gedaan aan de conclusie dat eiseres heeft voldaan aan de last.

25. Ook is geen sprake van schending van het evenredigheidsbeginsel door de opgelegde dwangsom. Gelet op hetgeen hiervoor is overwogen over de aard, omvang en context van de overtreding en de omstandigheid dat eiseres nalatig is geweest, acht de rechtbank de opgelegde last onder dwangsom niet onevenredig.

26. Verder is er geen reden om de last onder dwangsom in strijd met het gelijkheidsbeginsel te achten. Verweerder stelt terecht dat geen sprake is van gelijke gevallen met de in 2009 aan andere zorgverleners opgelegde dwangsommen, omdat het gevallen betrof uit een betrekkelijk ver verleden, die plaatsvonden vóór inwerkingtreding van de AVG. Daarnaast heeft verweerder toegelicht dat het ging om overtredingen van een duidelijk andere aard, namelijk het niet voldoen aan verplichtingen met een (voornamelijk) administratief karakter. Ook ging er in het geval van eiseres een ernstig beveiligingsincident aan de handhaving vooraf. Verweerder heeft terecht gesteld dat daarmee de context duidelijk anders is. Ook de onderzoeken bij ziekenhuizen in 2007 en 2012 waarnaar eiseres heeft verwezen, vonden plaats onder een andere wet en in een betrekkelijk ver verleden. Verder is hiervoor al overwogen dat het geval van de eerdergenoemde zorgverzekeraar geen gelijk geval betrof.

Conclusie

27. Gelet op hetgeen is overwogen over de hoogte van de boete zal de rechtbank het beroep gegrond verklaren. Het bestreden besluit komt voor wat betreft de hoogte van de boete wegens strijd met 5:46, tweede lid, van de Awb voor vernietiging in aanmerking. De rechtbank zal zelf in de zaak voorzien door het betreffende onderdeel van het primaire besluit te herroepen en de boete vast te stellen op een bedrag van € 350.000,-. De rechtbank zal bepalen dat deze uitspraak in zoverre in de plaats treedt van het vernietigde besluit.

28. Omdat de rechtbank het beroep gegrond verklaart, bepaalt de rechtbank dat verweerder aan eiseres het door haar betaalde griffierecht vergoedt.

29. De rechtbank veroordeelt verweerder in de door eiseres gemaakte proceskosten. Deze kosten stelt de rechtbank op grond van het Besluit proceskosten bestuursrecht voor de door een derde beroepsmatig verleende rechtsbijstand vast op € 2.136,- (1 punt voor het indienen van het bezwaarschrift, 1 punt voor het verschijnen ter hoorzitting, 1 punt voor het indienen van het beroepschrift, 1 punt voor het verschijnen ter zitting, met een waarde per punt van € 534,- en een wegingsfactor 1).

Beslissing

De rechtbank:

- verklaart het beroep gegrond;
- vernietigt het bestreden besluit voor zover het de hoogte van de boete betreft;
- herroept het primaire besluit in zoverre en bepaalt dat de bestuurlijke boete wordt vastgesteld op een bedrag van € 350.000,-;
- bepaalt dat deze uitspraak in zoverre in de plaats treedt van het vernietigde bestreden besluit;
- draagt verweerder op het betaalde griffierecht van € 354,- aan eiseres te vergoeden;
- veroordeelt verweerder in de proceskosten van eiseres tot een bedrag van € 2.136,-.

Deze uitspraak is gedaan door mr. R.H. Smits, voorzitter, en mr. D. Biever en mr. M.J.L. van der Waals, leden, in aanwezigheid van mr. M. de Graaf, griffier. De beslissing is in het openbaar uitgesproken op 31 maart 2021.

griffier voorzitter

Afschrift verzonden aan partijen op:

Rechtsmiddel

Tegen deze uitspraak kan binnen zes weken na de dag van verzending daarvan hoger beroep worden ingesteld bij de Afdeling bestuursrechtspraak van de Raad van State. Als hoger beroep is ingesteld, kan bij de voorzieningenrechter van de hogerberoepsrechter worden verzocht om het treffen van een voorlopige voorziening of om het opheffen of wijzigen van een bij deze uitspraak getroffen voorlopige voorziening.

Bijlage

Algemene Verordening Gegevensbescherming

Artikel 32:

1. 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'] voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

a. a) de pseudonimisering en versleuteling van persoonsgegevens;

b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;

c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;

d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

2. Bij de beoordeling van het passende beveiligingsniveau wordt 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.

3. Het aansluiten bij een goedgekeurde gedragscode als bedoeld in artikel 40 of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat dat de in lid 1 van dit artikel bedoelde vereisten worden nageleefd.

[...].

Artikel 58, tweede lid:

Elk toezichthoudende autoriteit heeft alle volgende bevoegdheden tot het nemen van corrigerende maatregelen:

[…]

d) de verwerkingsverantwoordelijke of de verwerker 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. 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; en

[…].

Artikel 83:

1. Elke toezichthoudende autoriteit zorgt 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.

2. Administratieve geldboeten worden, naargelang de omstandigheden van het concrete geval, opgelegd naast of in plaats van de in artikel 58, lid 2, onder a) tot en met h) en onder j), bedoelde maatregelen.

[…]

4. Inbreuken op onderstaande bepalingen zijn overeenkomstig lid 2 onderworpen aan administratieve geldboeten tot 10 000 000 EUR of, voor een onderneming, tot 2 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is:

a. a) de verplichtingen van de verwerkingsverantwoordelijke en de verwerker overeenkomstig de artikelen 8, 11, 25 tot en met 39, en 42 en 43;

[…].

Uitvoeringswet Algemene verordening gegevensbescherming

Artikel 14:

De Autoriteit persoonsgegevens kan 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.

Algemene wet bestuursrecht

Artikel 5:46:

1. De wet bepaalt de bestuurlijke boete die wegens een bepaalde overtreding ten hoogste kan worden opgelegd.

2. Tenzij de hoogte van de bestuurlijke boete bij wettelijk voorschrift is vastgesteld, stemt het bestuursorgaan de bestuurlijke boete af op de ernst van de overtreding en de mate waarin deze aan de overtreder kan worden verweten. Het bestuursorgaan houdt daarbij zo nodig rekening met de omstandigheden waaronder de overtreding is gepleegd.

[…].

Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg

Artikel 1:

In deze wet en de daarop berustende bepalingen wordt verstaan onder:

[…]

m. “Zorginformatiesysteem”: elektronisch systeem van een zorgaanbieder voor het verwerken van persoonsgegevens in een dossier, niet zijnde een elektronisch uitwisselingssysteem.

Artikel 15j, eerste lid:

Bij algemene maatregel van bestuur kunnen 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.

Besluit elektronische gegevensverwerking door zorgaanbieders

Ingevolge artikel 1 wordt in het Besluit 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.

Artikel 3, tweede lid:

Een zorgaanbieder draagt overeenkomstig het bepaalde in NEN 7510 en NEN 7512, zorg voor een veilig en zorgvuldig gebruik van het zorginformatiesysteem en een veilig en zorgvuldig gebruik van het elektronisch uitwisselingssysteem waarop hij is aangesloten.

Artikel 5, eerste lid:

De zorgaanbieder als verantwoordelijke voor een zorginformatiesysteem en de verantwoordelijke voor een elektronisch uitwisselingssysteem dragen er zorg voor dat de logging van het systeem voldoet aan het bepaalde in NEN 7513.

NEN 7510 en NEN 7513

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.

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.

Boetebeleidsregels 2019

Artikel 2:

2.1 De bepalingen ter zake van overtreding waarvan de Autoriteit Persoonsgegevens 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, zijn in bijlage 1 ingedeeld in categorie I, categorie II of categorie III.

2.2 De bepalingen ter zake van overtreding waarvan de Autoriteit Persoonsgegevens een bestuurlijke boete kan opleggen van ten hoogste het bedrag van € 20.000.000 of, voor een onderneming, tot 4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is, zijn in bijlage 2 ingedeeld in categorie I, categorie II, categorie III of categorie IV.

2.3 De Autoriteit Persoonsgegevens stelt 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, dan wel € 20.000.000 of, voor een onderneming, tot 4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is, vast binnen de volgende boetebandbreedtes: Categorie I Boetebandbreedte tussen € 0 en € 200.000 Basisboete: € 100.000 Categorie II Boetebandbreedte tussen € 120.000 en € 500.000 Basisboete: € 310.000 Categorie III Boetebandbreedte tussen € 300.000 en € 750.000 Basisboete: € 525.000 Categorie IV Boetebandbreedte tussen € 450.000 en € 1.000.000 Basisboete: € 725.000

2.4 De hoogte van de basisboete wordt vastgesteld op het minimum van de bandbreedte vermeerderd met de helft van de bandbreedte van de aan een overtreding gekoppelde boetecategorie.

Blijkens Bijlage 1 behorende bij artikel 2 is artikel 32 ingedeeld in categorie II.

Artikel 6:

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

Artikel 7:

Onverminderd de artikelen 3:4 en 5:46 van de Algemene wet bestuursrecht houdt de Autoriteit Persoonsgegevens rekening met de factoren genoemd onder a tot en met k, voor zover in het concrete geval van toepassing:

a. 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 of de verwerker genomen maatregelen om de door betrokkenen geleden schade te beperken;

[…].