AUTORITEIT
PERSOONSGEGEVENS

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

Aangetekend
[VERTROUWELIJK]

Datum	Ons kenmerk	Uw brief van
15 januari 2020	z2019-17017	29 juli 2019 (uw kenmerk: 232958)

Contactpersoon
[VERTROUWELIJK]

Onderwerp
Beslissing op bezwaar inzake boete en last onder dwangsom HagaZiekenhuis

Geachte [VERTROUWELIJK]

Hierbij ontvangt u het besluit van de Autoriteit Persoonsgegevens (AP) op uw bezwaarschrift van 29 juli 2019 en aangevuld bij brief en fax van 10 september 2019. Het bezwaar is gericht tegen het besluit van de AP van 18 juni 2019 (kenmerk: z2019-07604) tot oplegging van een bestuurlijke boete alsmede een last onder dwangsom aan uw cliënt Stichting HagaZiekenhuis (HagaZiekenhuis). Het besluit van 18 juni 2019 wordt hierna (ook) aangeduid als het primaire besluit.

1. Verloop van de procedure

1. De AP heeft op 4 april 2018 een melding van een datalek ontvangen van HagaZiekenhuis.

2. Naar aanleiding van vorenbedoelde melding heeft de AP een onderzoek ingesteld. In dat kader heeft op 31 oktober 2018 een onderzoek ter plaatse bij HagaZiekenhuis plaatsgevonden.[1]

3. Het onderzoek heeft in januari 2019 geresulteerd in een rapport van voorlopige bevindingen. Daarop heeft HagaZiekenhuis op 4 februari 2019 schriftelijk gereageerd.

4. Vervolgens heeft de AP - met inachtneming van de reactie van HagaZiekenhuis - het onderzoeksrapport definitief vastgesteld en bij brief van 26 maart 2019 aan HagaZiekenhuis doen toekomen.

[1] Ten aanzien van het verloop van het onderzoek wordt verwezen naar p. 2 en 3 van het primaire besluit alsmede naar paragraaf 1.2, p. 4 van het hierna genoemde definitieve onderzoeksrapport van de AP.

5. Bij brief van 4 april 2019 heeft de AP een voornemen tot het opleggen van een bestuurlijke boete en/of last onder dwangsom aan HagaZiekenhuis toegezonden. Op dat voornemen heeft HagaZiekenhuis zowel schriftelijk (bij brief van 18 april 2019) als mondeling (tijdens een hoorzitting op 25 april 2019) haar zienswijze gegeven.

6. Met inachtneming van de zienswijze van HagaZiekenhuis heeft de AP bij besluit van 18 juni 2019 besloten tot oplegging van zowel een bestuurlijke boete als een last onder dwangsom wegens overtreding van artikel 32, eerste lid, van de AVG.

7. Bij brief en fax van 29 juli 2019 heeft HagaZiekenhuis op nader aan te voeren gronden bezwaar gemaakt tegen vorenbedoeld besluit en verzocht om een termijn van 6 weken voor het aanvullen van gronden.

8. Bij brief van 31 juli 2019 heeft de AP HagaZiekehuis in de gelegenheid gesteld uiterlijk 11 september 2019 de gronden van bezwaar aan te vullen.

9. Bij brief en fax van 10 september 2019 alsmede bij brief en fax van 4 oktober 2019 heeft HagaZiekenhuis haar bezwaargronden aangevuld.

10. Op 16 oktober 2019 heeft een hoorzitting plaatsgevonden ten kantore van de AP. Van het horen is een verslag gemaakt. Dit verslag is als **bijlage** bij dit besluit gevoegd.

11. Op 17 oktober 2019 heeft een onderzoek ter plaatse plaatsgevonden ten kantore van HagaZiekenhuis te Den Haag om na te gaan of HagaZiekenhuis de last onder dwangsom heeft nageleefd.

12. Naar aanleiding van het verhandelde tijdens de hoorzitting op 16 oktober 2019 heeft HagaZiekenhuis bij brief, fax en e-mail van 5 november 2019 haar beroep op beperkte financiële draagkracht nader onderbouwd.

13. Bij brief van 2 december 2019 heeft de AP HagaZiekenhuis bericht dat HagaZiekenhuis ten tijde van het onderzoek ter plaatse van 17 oktober 2019 aan de last voldeed. [2]

14. Bij brief van 5 december 2019 heeft de AP u gevraagd of voormelde brief van de AP van 2 december 2019 voor HagaZiekenhuis aanleiding is de bezwaargronden tegen de last onder dwangsom in te trekken. In reactie daarop heeft u bij schrijven van 13 december 2019 aangegeven dat HagaZiekenhuis geen aanleiding ziet haar bezwaargronden ten aanzien van de last onder dwangsom in te trekken.

[2] Eerder, bij brief van 22 augustus 2019, heeft de AP al geconcludeerd dat door HagaZiekenhuis bij implementatie van de in haar brief van 9 augustus 2019 (kenmerk: 2019/0177/CvdW/PM/rv) vermelde voorgenomen maatregelen wordt voldaan aan het lastonderdeel dat betrekking heeft op de controle van logbestanden. Bij brieven van HagaZiekenhuis van 24 en 30 september 2019 (kenmerk: 2018/0109x/CvdW/PM/cb respectievelijk 2018/0109z/CvdW/JP/rv) heeft HagaZieknhuis uiteengezet op welke wijze zij uitvoering heeft gegeven aan de last.

2. Juridisch kader

15. Het relevante wettelijk kader is als bijlage opgenomen achteraan dit besluit.

3. Het primaire besluit

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

17. De AP heeft in het primaire besluit aan HagaZiekenhuis een bestuurlijke boete en een last onder dwangsom opgelegd wegens overtreding van artikel 32, eerste lid van de AVG in samenhang gelezen met artikel 3, tweede lid, van het Besluit elektronische gegevensverwerking door zorgaanbieders en het bepaalde onder 12.4.1 van NEN 7510-2 omdat niet is voldaan aan de eis van tweefactor authenticatie en de eis om regelmatig de logbestanden te beoordelen.

18. De hoogte van de bestuurlijke boete is vastgesteld op € 460.000. Hierbij heeft de AP zich gebaseerd op de Boetebeleidsregels Autoriteit Persoonsgegevens 2019 (Boetebeleidsregels 2019).[3]

19. Artikel 32 AVG is, zo volgt uit artikel 2.3 van de van de Boetebeleidsregels 2019, ingedeeld in categorie II. Hierbij geldt een boetebandbreedte van € 120.000 – € 500.000 en een zogenoemde basisboete van € 310.000. Deze basisboete geldt als (neutraal) uitgangspunt voor de verdere bepaling van de boetehoogte.[4] Die nadere bepaling stemt de AP vervolgens af op de factoren omschreven in artikel 7 van de Boetebeleidsregels 2019. Hierdoor kan de basisboete worden verhoogd of verlaagd.

20. In het primaire besluit vormde de factoren uit artikel 7, aanhef en onder a (aard, ernst en duur van de inbreuk) en b (opzettelijke/nalatige aard van de inbreuk), van artikel 7 van de Boetebeleidsregels 2019 de aanleiding de boete twee maal te verhogen met € 75.000.

21. Naast een bestuurlijke boete is aan HagaZiekenhuis ook een last onder dwangsom opgelegd vanwege dezelfde overtreding. De last strekt ertoe dat HagaZiekenhuis - binnen vijftien weken na dagtekening het primaire besluit - de toegang tot haar ziekenhuisinformatiesysteem uitsluitend mogelijk te maken met toepassing van tweefactor authenticatie, en dat de logbestanden regelmatig worden gecontroleerd op onrechtmatige toegang of onrechtmatig gebruik van patiëntgegevens. De hoogte van de dwangsom is daarbij vastgesteld op € 100.000 voor iedere twee weken na afloop van de begunstigingstermijn, tot een maximumbedrag van in totaal € 300.000.

[3] Stcrt. 2019, nr. 14586, 14 maart 2019.
[4] De hoogte van de basisboete kan worden berekend door het minimum - en het maximum bedrag van de desbetreffende bandbreedte bij elkaar op te tellen en vervolgens door twee te delen (vgl. art. 2.4 Boetebeleidsregels 2019).

4. Gronden van het bezwaar

22. Samengevat weergegeven heeft HagaZieknhuis de volgende bezwaargronden aangevoerd.

Geen gronden voor handhaving NEN-normen

Ontbreken juridische grondslag voor handhaving

23. HagaZiekenhuis meent dat de AP geen juridische grondslag heeft om handhavend op te treden. Anders dan de AP suggereert, volgt noch uit de AVG noch uit de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) dat de verplichting om 'passende maatregelen 'te nemen, dient te worden ingevuld aan de hand van de NEN-normen 7510, 7512 en 7513. Naar deze normen wordt verwezen in artikel 3, lid 2 en artikel 4 van het Besluit elektronische gegevensverwerking door zorgaanbieders (Begz).

24. De bevoegdheid om voor een bepaalde sector nadere regels te stellen voor de verwerking van persoonsgegevens (artikel 26 Wbp) is met de invoering van de AVG komen te vervallen. Hieruit volgt dat het wegvallen van de grondslag van het Begz, te weten artikel 26 Wbp, niet (uitsluitend) met artikel 15j Wabvpz kon worden hersteld. Daarmee is immers nog geen bevoegdheid aan de AP toegekend om voor een bepaalde sector nadere regels te stellen. De Wabvpz is dan ook geen uitwerking van de AVG, maar staat op zichzelf, naast de AVG en haar voorloper, de Wbp. De AP is niet bevoegd handhavend op te treden wegens vermeende overtreding van de NEN-normen op grond van het Begz/Wabvpz. Daartoe is slechts de Inspectie Gezondheidszorg en Jeugd bevoegd.

25. Uit paragraaf 2.4 van de memorie van toelichting op de UAVG volgt dat de materiële normen voor gegevensverwerking rechtstreeks uit de AVG volgen en niet langer op nationaal niveau mogen worden vastgelegd. De AP kan dan ook niet de open normen in de AVG invullen met nationale wet- en regelgeving, door middel van NEN-normen. HagaZiekenhuis verwijst daarbij naar overweging 8, 10 en 13 van de considerans van de AVG. De AVG verlangt van de lidstaten een autonome uitleg. De AP kan daarom geen boete of last onder dwangsom opleggen op grond van de (U)AVG wegens overtreding van de NEN-normen.

Strijd met het legaliteitsbeginsel

26. HagaZiekenhuis is verder van mening dat het bestreden besluit in strijd is met het legaliteitsbeginsel.

27. De AP kan slechts handhavend optreden vanwege het overtreden van de in artikel 32 van de AVG opgenomen open norm. Ten tijde van de vermeende overtreding was deze norm volgens HagaZiekenhuis niet nader ingevuld. Uit het in artikel 7 EVRM en artikel 5:4, lid 2, Awb vastgelegde legaliteitsbeginsel volgt dat de AP niet handhavend kon optreden. Een sanctie kan slechts worden opgelegd wegens een bij of krachtens wettelijk voorschrift verboden gedraging. Daarnaast dient dat voorschrift gelet op het lex certa-beginsel voldoende duidelijk, voorzienbaar en kenbaar te zijn. Dat is hier volgens HagaZiekenhuis niet het geval omdat de inhoud van de open norm in artikel 32, lid 1, AVG niet viel te kennen door een concrete toepassing in de praktijk. De AP had deze open norm eerst moeten verduidelijken. De verwijzing van de

AP naar een rapport van het College Bescherming Persoonsgegevens uit 2013 kan de AP niet baten omdat dit rapport gebaseerd is op de Wbp en de NEN-normen.

28. Ook het enkele feit dat HagaZiekenhuis de NEN-normen in haar beleid tot uitgangspunt heeft genomen, maakt nog niet dat de AP de naleving daarvan kan handhaven op de voet van de (U)AVG. Artikel 5:4, lid 2 Awb vereist een wettelijke grondslag. Intern beleid is onvoldoende.

29. Voor zover wel aan de NEN zou mogen worden getoetst, betoogt HagaZiekenhuis dat de AP heeft nagelaten om duidelijk te maken wanneer van 'regelmatig beoordelen van logbestanden' sprake is. HagaZiekenhuis heeft tijdens de zienswijzezitting uiteengezet hoe de controle op de logging binnen HagaZiekenhuis plaatsvindt en heeft de AP uitdrukkelijk gevraagd om een concrete invulling van de norm. Dat had voor de AP reden moeten zijn om deze norm te concretiseren. Het argument van de AP in paragraaf 5.2 van het bestreden besluit, waarin ze onderbouwt waarom door haar geen invulling is gegeven aan de norm 'regelmatig', gaat dus niet op omdat die erop neer komt dat de noodzaak van de omvang van controles afhankelijk is van de wijze waarop controle plaatsvindt. En de AP kende de wijze van controle.

30. HagaZiekenhuis vindt de NEN-7510-2 dermate vaag dat die vanwege strijdigheid met het legaliteits- en rechtszekerheidsbeginsel niet kan worden gehandhaafd met een boete of last onder dwangsom.

31. In haar brief van 4 oktober 2019 heeft HagaZiekenhuis nog aanvullend gemotiveerd waarom ze meent dat de AVG geen ruimte biedt om artikel 32 AVG nader in te vullen door middel van NEN-normen. Ze verwijst daarbij naar jurisprudentie van het Hof van Justitie van de EG waaruit volgt dat lidstaten geen bepalingen, materiële voorschriften of bindende uitleggingsbepalingen mogen toevoegen aan een verordening.[5] De AP doet dat volgens HagaZiekenhuis wel door de NEN-normen (die nationale normen zijn) toe te passen. Dit staat een uniforme toepassing van de AVG in de EU in de weg. De AVG kent geen bepaling die het mogelijk maakt om nadere nationale regels te stellen ten aanzien van artikel 32 AVG.[6]

Bezwaren tegen boetehoogte en hoogte van de dwangsom

HagaZiekenhuis niet nalatig geweest

32. HagaZiekenhuis stelt niet nalatig te zijn geweest. In dit verband wijst ze op de volgende getroffen maatregelen:
    - Er komt een extra waarschuwing in beeld als een medewerker een dossier opent;
    - Er is een verplichte e-learning cursus voor alle medewerkers die toegang hebben tot het elektronische patiëntendossier;
    - Alle medewerkers worden in een persoonlijke brief gewezen op het beroepsgeheim en het belang van vertrouwelijkheid van patiëntgegevens;
    - Er wordt extra informatie gegeven bij de introductiebijeenkomst voor nieuwe medewerkers;
    - De arbeidsovereenkomst is aangescherpt;

[5] HvJEG 18 februari 1970 (Bollmann, 40/69), HvJEG 6 juli 1972 (Schlüter & Maack) HvJEG 10 oktober 1973 (Variola, 34/73) en HvJEG 31 januari 1978 (Fratelli Zerbone, 94/77).
[6] In dat kader verwijst HagaZiekenhuis naar de uitspraak van HvJEG 11 januari 2001 (Azienda Agricola Monte Arcosu, C-403/98).

- Er is een mogelijkheid voor patiënten om hun patiëntgegevens extra af te schermen;
- Waar mogelijk worden autorisaties aangescherpt;
- Er wordt gewerkt aan een maatwerkoplossing voor de controle op de logging.[7]

33. HagaZiekenhuis geeft verder aan dat de conclusie dat ze nalatig is geweest, niet juist is omdat de AP eraan voorbij gaat dat het implementeren van tweefactor authenticatie geen maatregel is die onbevoegde inzage in patiëntendossiers door medewerkers kan voorkomen. Na het inloggen met tweefactor authenticatie is het immers nog steeds mogelijk dat medewerkers onbevoegd in een patiëntendossier kijken.

34. Ook merkt HagaZiekenhuis op dat de stelling van de AP, dat de door HagaZiekenhuis getroffen maatregelen niet zien op het regelmatig controleren van de logging, niet juist is. HagaZiekenhuis heeft, zoals is vastgelegd in het verslag van de zienswijze zitting, het aantal steekproeven verhoogd van vier naar zes.
In dit verband merkt HagaZiekenhuis verder op dat het in strijd is met de beginselen van behoorlijk bestuur in het algemeen en het rechtzekerheidsbeginsel in het bijzonder om een bestuurlijke boete op te leggen op basis van een onduidelijke norm (de NEN-norm ten aanzien van logging is open) en die norm door het bestuursorgaan niet is geconcretiseerd.

AP heeft HagaZiekenhuis ten onrechte dubbel beboet

35. Door de AP is aan HagaZiekenhuis een basisboete opgelegd van € 310.000,-. Deze basisboete is door de AP vervolgens twee maal verhoogd met een bedrag van € 75.000,- omdat er volgens de AP sprake is van "een structurele overtreding die nog steeds voortduurt". De onderbouwing van de AP voor de eerste verhoging van de basisboete komt op hetzelfde neer als de onderbouwing voor de tweede verhoging. De door de AP geconstateerde voortdurende overtreding is immers het gevolg van het feit dat HagaZiekenhuis geen of onvoldoende maatregelen genomen heeft. Het is volgens HagaZiekenhuis niet in overeenstemming met de Boetebeleidsregels en het is ook niet redelijk om de basisboete twee keer te verhogen vanwege hetzelfde feit. De dubbele verhoging is daarmee ook in strijd met het ne bis in idem-beginsel (artikel 5:43 Awb).

Boete ten onrechte niet verlaagd

36. Artikel 7, aanhef en onder c, van de Boetebeleidsregels geeft de AP de mogelijkheid om de basisboete te verlagen als er door de verwerkingsverantwoordelijke maatregelen zijn genomen om de door de betrokkenen geleden schade te beperken. In dit verband wordt door HagaZiekenhuis gewezen op de getroffen maatregelen.

37. De boete die de AP aan HagaZiekenhuis oplegt, gaat rechtstreeks ten koste van de (schaarse) middelen die voor patiëntenzorg kunnen worden ingezet. Daarmee gaat de boete ten koste van de mogelijkheid om te investeren in de zorg en te innoveren, op basis waarvan HagaZiekenhuis in staat blijft om duurzaam zorg

[7] Deze maatwerkoplossing (een speciaal voor HagaZiekenhuis ontwikkelde softwaretoepassing genaamd [VERTROUWELIJK]) is inmiddels doorgevoerd en actief. Verwezen zij naar de brief van HagaZiekenhuis van 24 september 2019 (kenmerk: 2018/0109x/CvdW/PM/cb) alsmede naar de brief van de AP van 2 december 2019 waarin de bevindingen staan naar aanleiding van het onderzoek ter plaatse op 17 oktober 2019 ter controle van het voldoen aan de last.

te leveren. HagaZiekenhuis meent ook om deze reden dat een verlaging van de basisboete gerechtvaardigd is.

38. HagaZiekenhuis doet tot slot nog een beroep op verminderde financiële draagkracht en verzoekt om die reden om boetematiging. In dit verband wijst HagaZiekenhuis in haar brief van 5 november 2019 op een rapport van accountantskantoor [VERTROUWELIJK] en een rapport van het financieel strategisch adviesbureau [VERTROUWELIJK], en verwijst ze verder naar de financiële cijfers van HagaZiekenhuis over 2019.

Dwangsom te hoog vastgesteld

39. De AP heeft aan de last een dwangsom verbonden van € 100.000 voor iedere twee weken dat niet (geheel) aan de last is voldaan, tot een maximumbedrag van in totaal € 300.000. HagaZiekenhuis stelt zich op het standpunt dat deze bedragen niet in verhouding staan tot de verweten gedraging. Daarmee is het besluit in strijd met het evenredigheidsbeginsel in de zin van artikel 3:4 Awb en eveneens met de specifieke bepaling in artikel 5:32b, lid 3, Awb.

40. De last onder dwangsom gaat ten koste van de mogelijkheid om te investeren in de zorg en te innoveren. Dat kan de bedoeling niet zijn van handhaving. HagaZiekenhuis meent ook om die reden dat een verlaging van de dwangsom gerechtvaardigd is.

41. De hoogte van de dwangsom is in strijd met het gelijkheidsbeginsel. De AP heeft sinds de inwerkingtreding van de AVG diverse lasten onder dwangsom opgelegd. De dwangsom die aan HagaZiekenhuis is opgelegd, is veruit het hoogste.

42. De dwangsom is in strijd met het evenredigheidsbeginsel, omdat één dwangsombedrag is verbonden aan een last die uit twee onderdelen bestaat. Dit betekent dat HagaZiekenhuis ook dwangsommen verbeurt als onderdeel 1 wel wordt nageleefd, maar onderdeel 2 niet. Dit is volgens HagaZiekenhuis onredelijk.

5. Oordeel AP

43. HagaZiekenhuis verwerkt in haar ziekenhuisinformatiesysteem op elektronisch wijze en op grote schaal (medische) persoonsgegevens. Het gaat (veelal) om uiterst gevoelige gegevens over gezondheid. Deze gegevens kwalificeren als een bijzondere categorie van persoonsgegevens in de zin van artikel 9, eerste lid, AVG waarvoor in beginsel een verwerkingsverbod geldt tenzij sprake is van een uitzondering als vermeld in de AVG en UAVG. Voor het vertrouwen van patiënten in een zorgverlener is het van groot belang dat met deze persoonsgegevens uiterst zorgvuldig wordt omgegaan en dat ze adequaat worden beveiligd. Ziekenhuispatiënten - die zich veelal in een kwetsbare positie bevinden - moeten er steeds op kunnen vertrouwen dat er vertrouwelijk met hun persoonsgegevens wordt omgegaan en dat wordt voorkomen dat medewerkers, die geen behandelrelatie hebben met de patiënt of die gegevens niet nodig hebben voor de beheersmatige afwikkeling van de zorgverlening of behandeling, onbevoegd patiëntendossiers kunnen raadplegen. Tegen deze achtergrond heeft de AP onderzoek gedaan bij HagaZiekenhuis. Naar aanleiding van de uitkomsten van dat onderzoek is in het primaire besluit vastgesteld dat HagaZiekenhuis geen, dan

wel onvoldoende passende technische en organisatorische maatregelen heeft genomen als bedoeld in artikel 32, eerste lid, van de AVG en is een bestuurlijke boete en een last onder dwangsom opgelegd. In onderhavige beslissing op bezwaar komt de AP naar aanleiding van de door u aangevoerde bezwaargronden niet tot een andersluidend oordeel.

Passende maatregelen; tweefactor authenticatie en controle op de logging

44. De overtreding van artikel 32, eerste lid, AVG omvat twee aspecten. Het eerste betreft het niet voldoen aan het vereiste van tweefactor authenticatie. Gebleken is dat het voor gebruikers van het ziekenhuisinformatiesysteem mogelijk was 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 één factor authenticatie.[8] Het ziekenhuisinformatiesysteem van HagaZiekenhuis had niet de ingebouwde verplichting, maar alleen de mogelijkheid om met tweefactor authenticatie in te loggen. Daarmee had HagaZiekenhuis niet op een juiste wijze de eis van tweefactor authenticatie in haar bedrijfsvoering geïmplementeerd.[9]Dit is door HagaZiekenhuis ook erkend.[10]

45. De tweede reden waarom artikel 32, eerste lid, AVG is overtreden, houdt verband met het niet regelmatig controleren van de logging van de toegang tot de patiëntendossiers. 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 HagaZiekenhuis voorzag in een controle op de logging van een aselecte steekproef van jaarlijks zes patiëntdossiers.[11] In de relevante periode waarop het onderzoek van de AP zag - januari 2018 tot en met oktober 2018 - is er proactief één controle op ongeautoriseerde inzage geweest[12] en 6 controles op verzoek van patiënten en medewerkers.[13] [14]

46. Eén controle in de periode van januari 2018 tot en met oktober 2018 kan, afgezet tegen het aantal patiëntbezoeken [15]dat HagaZiekenhuis jaarlijks krijgt en in 2017 (afgerond) uitkwam op 381.500[16] en het

[8] Over het algemeen worden drie factoren onderscheiden: iets dat de gebruiker weet (een wachtwoord of pincode); iets dat de gebruiker heeft (bijvoorbeeld een token); of iets dat de gebruiker is (een biometrisch gegeven). (Bron: NCSC, Gebruik tweefactor-authenticatie. Wachtwoorden alleen zijn niet altijd voldoende. Factsheet FS-2015-02, versie 1.1. 22 oktober 2018).
[9] Vgl. p. 11, paragraf 2.3 Onderzoeksrapport AP, maart 2019
[10] Zie de Brief HagaZiekenhuis 4 februari 2019 (kenmerk: 2018/109j/CvdW/PM/rv), p. 2 onder het kopje 'Authenticatie' en ook verslag van de hoorzitting naar aanleiding van het bezwaarschrift, p. 6. Sinds 30 september 2019 past HagaZiekenhuis de tweefactor authenticatie op de juiste wijze toe. (Vgl. brief HagaZiekenhuis 30 september 2019 (kenmerk: 2018/0109z/CvdW/JP/rv).
[11] Brief HagaZiekenhuis, 23 oktober 2018 (kenmerk: 2018/0109c/RdF/PM/rv), antwoord op vraag 5 en Bijlage 3: Autorisatie Digitale Patiënten Dossiers.
HagaZiekenhuis (versie 1.0, mei 2018), p. 3 en 6.
[12] Met betrekking tot het dossier van de bekende Nederlander.
[13] Vgl. brief HagaZiekenhuis, 23 oktober 2018 (kenmerk: 2018/0109c/RdF/PM/rv), antwoord op vraag 5.
[14] Thans bedraagt het aantal steekproeven 132 per jaar. Zie daarover nader het rapport van bevindingen van 2 december 2019 naar aanleiding van het onderzoek ter plaatse naar de naleving van de last onder dwangsom op 17 oktober 2019.
[15] Welke bezoeken steeds resulteren in raadpleging van een patiëntendossier.
[16] In 2017 ging het om 381.500 patiëntbezoeken. Vgl. de bijlage bij brief HagaZiekenhuis van 9 augustus 2019 (kenmerk: 2019/0177/CvdW/PM/rv). Verder wijst de AP op de door HagaZiekenhuis ter zienswijzezitting overgelegde cijfers uit het Jaarverslag. Het gaat in totaal om (afgerond) 381.500 patiëntbezoeken in 2017, die zijn onderverdeeld in 28.500 opnamen, 158.000 eerste polikliniekbezoeken, 52.000 eerste hulp consulten en 143.000 verpleegdagen.

aantal medewerkers dat (potentieel) toegang tot de patiëntendossiers heeft[17], naar het oordeel van de AP niet worden beschouwd als 'regelmatige' controle en daarmee niet als een passende maatregel in de zin van artikel 32, eerste lid, van de AVG. Daarbij merkt de AP op dat de in die periode door HagaZiekenhuis uitgevoerde reactieve controles evenmin - zelfstandig noch in combinatie met de proactieve controle van het patiëntendossier van de bekende Nederlander - kunnen worden beschouwd als regelmatige controle. Dergelijke reactieve controles zijn immers louter afhankelijk van een (uitdrukkelijk) verzoek van een patiënt of medewerker.[18]

47. Ook de zes (proactieve) controles op de logging die HagaZiekenhuis heeft aangekondigd[19] en uitgevoerd[20] in 2019 acht de AP, wederom afgezet tegen het aantal patiëntbezoeken - die steeds resulteren in raadpleging van een patiëntendossier[21] - en het aantal medewerkers, onvoldoende om als regelmatig te kunnen worden aangemerkt.

Consistente uitleg 'passende maatregelen' onder de Wbp en de AVG

48. Zowel de eis van tweefactor authenticatie als de eis van de controle op de logging zijn niet nieuw. Het gaat om een voortzetting van de wijze waarop ook onder het oude regime van Richtlijn 95/46/EG en de Wbp uitvoering is gegeven aan wat werd gezien als 'passende maatregelen' en is ontleend aan de NEN-norm 7510-2.[22]Deze uitleg heeft de AP gecontinueerd in het kader van de uitleg van artikel 32, eerste lid, AVG en is daar ook steeds transparant over geweest.[23] De AP is van oordeel dat deze uitleg ook onder de AVG een correcte uitleg is van de norm 'passende maatregelen' uit artikel 32, eerste lid, AVG. Omdat HagaZiekenhuis niet conform deze uitleg heeft gehandeld, vindt de AP het opleggen van handhavende maatregelen opportuun. Hierna zal de AP haar standpunt tegen de achtergrond van de bezwaren van HagaZiekenhuis nader motiveren.

6. Heroverweging

49. De AP beoordeelt ingevolge artikel 7:11 van de Awb op grond van uw bezwaar of zij bij het primaire besluit terecht tot de oplegging van de last onder dwangsom en een bestuurlijke boete is overgegaan.

---

[17] Tijdens de hoorzitting (p. 6 hoorzittingsverslag) heeft HagaZiekenhuis verklaard dat er 3.500 mensen werkzaam zijn bij HagaZiekenhuis.
[18] De AP merkt in dit verband op dat de door HagaZiekenhuis uitgevoerde controle ook niet in overeenstemming is met haar eigen autorisatiebeleid.
[19] Verklaring [VERTROUWELIJK], 31 oktober 2018 zoals weergegeven in het verslag van ambtshandelingen d.d. 19 december 2018, bijlage 3, pagina 4-5 en Reactie HagaZiekenhuis d.d. 23 oktober 2018, Bijlage 19: Procedure Steekproef Logging en Planning Steekproef Logging.
[20] Verslag zienswijzezitting. P.2, welk verslag als bijlage is bijgevoegd bij de brief van de AP van 16 mei 2019 (kenmerk:z2019-07604).
[21] Een steekproef van 6 gerelateerd aan 381.000 patiëntenbezoeken (en daarmee minstens evenzoveel dossierraadplegingen) komt dan neer op 0,0016%.
[22] In juni 2013 heeft de AP hierover een onderzoeksrapport gepubliceerd; https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-zorginstellingen-onzorgvuldig-met-medische-gegevens
[23] Vgl.: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/gezondheid/zorgverleners-en-de-avg?qa=nen%207510&scrollto=1 en https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/gezondheid/zorgverleners-en-de-avg#welke-norm-hanteert-de-ap-als-het-gaat-om-de-beveiliging-van-patiëntgegevens-7366.

Bevoegdheid, artikel 32 AVG en lex certa

Bevoegdheid

50. HagaZiekenhuis stelt dat de AP het opleggen van een boete en een last onder dwangsom alleen kan baseren op grond van de AVG en de UAVG en niet op grond van de Wabvpz en het daarop gebaseerde Begz, met de daarin opgenomen NEN-normen.

51. Dienaangaande merkt de AP het volgende op. In het primaire besluit is vastgesteld dat HagaZiekenhuis de (beveiligings)norm zoals neergelegd in artikel 32, eerste lid, AVG heeft overtreden omdat onvoldoende passende technische en organisatorische maatregelen zijn genomen teneinde een op het risico afgestemd beveiligingsniveau voor de verwerking van persoonsgegevens te waarborgen. Het is dus die norm uit artikel 32, eerste lid, van de AVG waarvan de AP heeft geconstateerd dat die is overtreden door HagaZiekenhuis.[24] In het primaire besluit wordt weliswaar overwogen dat artikel 32 van de AVG in samenhang moet worden gelezen met artikel 3, tweede lid, van het Begz en het bepaalde onder 12.4.1 van NEN 7510-2, maar daaruit kan niet de conclusie worden getrokken dat de Begz dan wel de NEN normen worden aangemerkt als de overtreden voorschriften op grond waarvan de AP is overgegaan tot opleggen van handhavende maatregelen.[25] Dat is ook niet het geval. Wél vormen in onderhavige casus de in de NEN 7510-2 vervatte eis van tweefactor authenticatie alsmede de eis om logbestanden regelmatig te beoordelen, de concrete invulling/interpretatie van wat in dit geval als 'passende technische en organisatorische maatregelen' in de zin van artikel 32, eerste lid, AVG hebben te gelden. De AP heeft de boete en de last onder dwangsom dus ook niet opgelegd op grond van en vanwege een overtreding van de Wabvpz en/of de Begz en de daarin opgenomen NEN-normen, maar op grond van het niet nemen van passende technische en organisatorische maatregelen in de zin van artikel 32, eerste lid, AVG.

52. In haar bij brief van 4 oktober 2019 nader aangevulde bezwaarschrift wijst HagaZiekenhuis nog op Europeesrechtelijke jurisprudentie[26] Deze jurisprudentie ziet in de kern op het verbod om nadere (bindende) regels te stellen in nationale regelgeving in het geval er een Europese verordening geldt. Een dergelijke situatie doet zich in casu evenwel niet voor. Nadere regels zijn niet gesteld. Dat neemt niet weg dat in een concreet geval artikel 32 AVG wel moet worden toegepast en geïnterpreteerd. De toepassing en interpretatie is - gelet op de haar in artikel 6, derde lid, UAVG opgedragen taak om toezicht te houden op de naleving van de AVG - aan de AP. Dat is dan ook wat de AP heeft gedaan en waartoe ze gehouden is. Het is uiteindelijk aan de nationale rechter en het Hof van Justitie van de EU om te beoordelen of de AP de

[24] Op grond van artikel 58, tweede lid, aanhef en onder d en i, van de UAVG, in samenhang met artikel 83, vierde lid, aanhef en onder a, van de AVG en artikel 14, derde lid, van de UAVG is de AP bevoegd om een bestuurlijke boete en een last onder dwangsom op te leggen als sprake is van overtreding van artikel 32, eerste lid, van de AVG.
[25] In dit verband merkt de AP overigens op dat HagaZiekenhuis is gebonden aan de Begz en daarmee, gelet op artikel 3, tweede lid, Begz, wettelijk verplicht is aan de daarin genoemde NEN-normen. Dat, naar HagaZiekenhuis stelt in haar bezwaarschrift, de bevoegdheid om voor een bepaalde sector nadere regels te stellen voor de verwerking van persoonsgegevens (artikel 26 Wbp) met de invoering van de AVG is komen te vervallen, weerspreekt de AP. Naar het oordeel van de AP biedt artikel 6, tweede lid en of derde lid, AVG, daartoe juist uitdrukkelijk wel de mogelijkheid.
[26] HvJ EG 18 februari 1970, zaak 40-69 (Bollmann), HvJ EG 6 juni 1972, zaak 94-71 (Schütler & Maack), HvJ EG 10 oktober 1973, zaak 34-73 (Fratelli Variola), HvJ EG 31 januari 1978, zaak 94/77 (Fratelli Zerbone)

door haar gegeven interpretatie van de normen uit de AVG rechtens juist is.[27] Daarmee wordt een autonome uitleg geborgd.

Artikel 32 AVG en lex certa

53. Ten aanzien van de stelling van HagaZiekenhuis dat het primaire besluit in strijd is met het in het legaliteitsbeginsel vervatte lex certa-beginsel omdat - zoals HagaZiekenhuis betoogt - sprake zou zijn van een vage norm, overweegt de AP als volgt.

54. Het lex certa-beginsel verlangt van de wetgever dat hij met het oog op de rechtszekerheid op een zo duidelijk mogelijke wijze een norm of verboden gedraging omschrijft.[28] Iemand moet kunnen weten ter zake van welke gedraging of nalaten hij kan worden gestraft. Dat vereist dat de invulling van een wettelijke bepaling voldoende duidelijk, bepaald en kenbaar dient te zijn. Dat betekent echter niet dat het gebruik van een vage - of open norm niet mogelijk is. Integendeel, de wetgever kan volstaan met dergelijke normen. Open normen kunnen noodzakelijk en daarmee aanvaardbaar zijn omdat het recht ook moet kunnen functioneren bij gewijzigde omstandigheden.[29] In het zogenoemde Krulsla-arrest oordeelde de Hoge Raad dat het bij het omschrijven van delicten, gebruik maken van een zekere vaagheid, bestaande in het bezigen van algemene termen, soms onontkoombaar is om te voorkomen dat gedragingen die strafwaardig zijn buiten het bereik van de delictsomschrijving vallen.[30] Niet altijd kan worden voorzien op welke wijze de te beschermen belangen in de toekomst zullen worden geschonden en omdat, indien dit wel is voorzien, delictsomschrijvingen anders te verfijnd worden met als gevolg dat de overzichtelijkheid wegvalt en daarmee het belang van de algemene duidelijkheid van de wetgeving schade lijdt. Naast de Hoge Raad geven ook de (hoogste) bestuursrechters op deze wijze invulling aan het lex certa-beginsel.[31]

55. Ten aanzien van de vraag of de desbetreffende norm uit artikel 32, eerste lid, AVG (de plicht tot het treffen van 'passende technische en organisatorische maatregelen') strijdig is met het lex certa-beginsel, merkt de AP het volgende op.

56. Allereerst moet blijkens de tekst van artikel 32, eerst lid, AVG bij de te treffen maatregelen rekening worden gehouden 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. Verder wordt in artikel 32, eerste lid, aanhef, en onderdelen a-d, AVG een nadere concretisering gemaakt van wat de 'passende technische en organisatorisch maatregelen' onder meer omvat[32]:

[27] Vgl. Tweede Kamer, vergaderjaar 2017–2018, 34 851, nr. 3, p. 53
[28] Het lex certa-beginsel is vastgelegd in artikel 5:4 Awb, artikel 7 EVRM en artikel 15 IVBPR alsmede in artikel 49 van het Handvest van de grondrechten van de Europese Unie.
[29] EHRM, Kokkinakis vs. Griekenland, arrest van 25 mei 1993, 14307/88.
[30] HR, arrest van 31 oktober 2000, ECLI:NL:HR:2000:AA7954, rov. 3.4.
[31] Zie bijv. ABRvS 9 juli 2014 (ECLI:NL:RVS:2014:2493), CBb 22 februari 2012 (ECLI:NL:CBB:2012:BV6713) en CRvB 8 januari 2019 (ECLI:NL:CRVB:2019:26).
[32] Artikel 32 AVG omvat een meer specifiekere uitwerking van het (algemene) beginsel van integriteit en vertrouwelijkheid zoals vastgelegd in artikel 5, eerste lid, aanhef en onder f, AVG.

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.

Het tweede lid van artikel 32 AVG bepaalt verder dat bij de beoordeling van het passende beveiligingsniveau met name rekening wordt gehouden met de verwerkingsrisico's als gevolg van ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

57. Aldus geeft artikel 32, AVG, mede in samenhang met de considerans[33], al een nadere duiding aan de norm 'passende technische en organisatorische maatregelen' en wordt aangegeven waarmee specifiek rekening moet worden gehouden. Daaronder begrepen het 'garanderen van de integriteit'[34] en 'ongeoorloofde toegang'[35]. De eisen van tweefactor authenticatie en regelmatige controle van de logging vormen een nadere uitwerking/invulling van die begrippen. In het licht van het vorenstaande is, naar het oordeel van de AP, het eisen van tweefactor authenticatie en regelmatige controle van logging in het kader van het nemen van passende technische en organisatorische maatregelen ten einde ongeoorloofde toegang te voorkomen dan wel te belemmeren, dan ook redelijkerwijs voorzienbaar. Daarbij moet worden bedacht dat artikel 32 AVG voorziet in een norm die zich richt tot alle verwerkingsverantwoordelijken, ongeacht in welk marksegment die actief zijn. De AVG beoogt dus alle gebieden en alle vormen van gegevensverwerking te bestrijken. Alle verwerkingsverantwoordelijken dienen deze norm dus in acht te (kunnen)nemen. Verder moeten de te treffen maatregelen in overeenstemming zijn met de stand der techniek. Om daar zinvol uitvoering aan te kunnen geven, is het gedetailleerd voorschrijven van die maatregelen niet mogelijk gelet op de snelheid waarmee de techniek in de huidige sterk gedigitaliseerde maatschappij voortschrijdt. Met de zich snel ontwikkelende techniek zal dus periodiek een nieuwe afweging moeten (kunnen) worden gemaakt. Dat vraagt om (een zekere mate van) flexibiliteit en toekomstbestendigheid van de norm, en dat rechtvaardigt dat – tegen de achtergrond van de hiervoor

[33] Overweging 83 van de considerans van de AVG komt tekstueel in hoge mate overeen met wat er in artikel 32 AVG staat:
Teneinde de veiligheid te waarborgen en te voorkomen dat de verwerking inbreuk maakt op deze verordening, dient de verwerkingsverantwoordelijke of de verwerker de aan de verwerking inherente risico's te beoordelen en maatregelen, zoals versleuteling, te treffen om die risico's te beperken. Die maatregelen dienen een passend niveau van beveiliging, met inbegrip van vertrouwelijkheid, te waarborgen, rekening houdend met de stand van de techniek en de uitvoeringskosten afgezet tegen de risico's en de aard van de te beschermen persoonsgegevens. Bij de beoordeling van de gegevensbeveiligingsrisico's dient aandacht te worden besteed aan risico's die zich voordoen bij persoonsgegevensverwerking, zoals de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot de doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig, hetgeen met name tot lichamelijke, materiële of immateriële schade kan leiden.
[34] Artikel 32, eerste lid, aanhef, en onderdeel b, AVG.
[35] Artikel 32, tweede lid, AVG.

aangehaalde onder randnummer 52 opgesomde jurisprudentie – in dit geval sprake is van (meer) open normen zoals die zijn opgenomen in artikel 32 van de AVG.[36]

58. Ten aanzien van de vraag of de uitleg die de AP heeft gegeven aan de norm 'passende technische en organisatorische maatregelen' voldoende duidelijk, bepaald en kenbaar is, is verder het volgende van belang. In het algemeen geldt dat de materiële normen waaraan de verwerking van persoonsgegevens onder het regime van de AVG moet voldoen, in grote lijnen gelijk zijn gebleven aan die uit de richtlijn 95/46/EG en de Wbp.[37] Specifiek ten aanzien van de bewoordingen 'passende technische en organisatorische maatregelen' - zoals opgenomen in artikel 32 AVG - is sprake van een voortzetting van wat ook al gold onder Richtlijn 95/46/EG en de Wbp.[38] 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, 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 worden gehandhaafd.[39] 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.[40] In vergelijkbare zin heeft ook de AVG-Helpdesk voor Zorg, Welzijn en Sport dit gecommuniceerd. [41]

59. Gelet op het vorenstaande is de AP is van mening dat de Europese wetgever heeft kunnen volstaan met de in artikel 32 AVG neergelegde norm ten aanzien van de te nemen passende technische en organisatorische maatregelen.

Norm 'regelmatige controle' nader bezien

60. Specifiek ten aanzien van de eis van de regelmatige controle op de logging en het bezwaar van HagaZiekenhuis dat deze norm te vaag is, merkt de AP aanvullend nog het volgende op. De AP is van oordeel dat de (proactieve) controle op de logging in de periode van januari 2018 tot en met oktober 2018

---

[36] In dit kader wijst de AP nog op de memorie van toelichting bij artikel 13 van de Wbp (de voorloper van artikel 32 AVG): *(...)"In het begrip <<passende>> ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek. Dit is in eerste aanleg een vraag van professionele ethiek van personen belast met de informatiebeveiliging. De normen van deze ethiek worden in deze bepaling van een juridisch sluitstuk voorzien, in die zin dat daaraan een wettelijke verplichting voor de verantwoordelijke is verbonden. Het is niet aan de wetgever om nadere details te geven over de aard van de beveiliging. Dergelijke details zouden sterk tijdgebonden zijn en daarmee afbreuk doen aan het nagestreefde niveau van beveiliging. "(...).* (onderstreping toegevoegd door de AP). Zie TK 1997-1998, 25 892, nr. 3, p. 98-99.

[37] Blijkens overweging 9 van de considerans bij de AVG blijven de doelstellingen en beginselen van richtlijn 95/46/EG overeind.

[38] 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.

[39] 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

[40] Vgl.: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/gezondheid/zorgverleners-en-de-avg?qa=nen%207510&scrollto=1 en https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/gezondheid/zorgverleners-en-de-avg#welke-norm-hanteert-de-ap-als-het-gaat-om-de-beveiliging-van-patiëntgegevens-7366

[41] Vgl.: https://www.avghelpdeskzorg.nl/onderwerpen/beveiliging/nen-7510. Deze helpdesk is een samenwerking tussen koepelorganisaties in de zorg, het sociaal domein, NOC*NSF en het ministerie van Volksgezondheid, Welzijn en Sport.

van één dossier (met betrekking tot het dossier van de bekende Nederlander)[42] afgezet tegen de 381.500[43] patiëntbezoeken en bijbehorende dossierraadplegingen bij het HagaZiekenhuis in 2017 (evident) niet als 'regelmatig' kan worden gekwalificeerd. Dat geldt evenzeer voor de - ten tijde van de oplegging van de bestuurlijke boete aangekondigde[44] en deels uitgevoerde[45] - steekproefsgewijze controle op de logging van zes dossiers over 2019. Het idee erachter is dat er *doorlopend* voldoende acht wordt geslagen op de in het ziekenhuis aanwezige aantal patiënten en medewerkers. Dat genereert een verwerking van zeer grote hoeveelheden data. HagaZiekenhuis heeft te maken met een groot aantal patiëntenbezoeken en heeft veel medewerkers die (in potentie) allemaal toegang kunnen krijgen tot de patiëntendossiers.[46] Het 'open' karakter van een ziekenhuis in ogenschouw nemende (iedereen kan een ziekenhuis bezoeken; bekende en onbekende patiënten), de gevoeligheid van de persoonsgegevens en het feit dat er goede zorg geleverd dient te worden waardoor toegang tot - en daarmee verwerking van - medische gegevens geen belemmering mag zijn, maakt (juist) dat een regelmatige controle op de logging die in verhouding staat tot het aantal dossiers en dossierraadplegingen noodzakelijk is voor een goede beveiliging. Een (handmatige) steekproef van 6 patiëntendossiers getuigt naar het oordeel van de AP niet van voldoende gevoel van urgentie en duidt er niet op dat HagaZiekenhuis op dit vlak 'in control' is. Haga beschikte niet over een automatisch georganiseerd controle proces, maar hanteerde een handmatige controle die bovendien op zeer incidentele basis werd uitgevoerd. Deze werkwijze sluit als gezegd niet goed aan bij het grote aantal patiëntenbezoeken/dossierraadplegingen en het daarmee gepaard gaande risico van mogelijk onbevoegde dossierraadplegingen. Naar het oordeel van de AP kan daarom niet worden gesproken van een passende maatregel. Dat had ook HagaZiekenhuis moeten beseffen en duidelijk moeten zijn gelet op de norm die de AP ook voor de inwerkingtreding van de AVG al hanteerde. Bezien tegen die achtergrond is van een te vage/onduidelijke norm, zoals HagaZiekenhuis stelt, geen sprake.

61. Dat de AP niet op voorhand heeft aangegeven hoeveel dossiers in het geval van HagaZiekenhuis dan wél moeten worden beoordeeld, betekent nog niet dat, zoals HagaZieknhuis betoogt, daarmee dus de norm te vaag is en sprake is van een schending van het legaliteits- of het rechtszekerheidsbeginsel. Hoeveel dossiers moeten worden beoordeeld, is mede afhankelijk van de feiten en omstandigheden van de concrete situatie, zoals het aantal loggingen in relatie tot het aantal patiëntendossiers en het aantal medewerkers dat toegang kan krijgen, en kan dus per geval anders zijn. Daarbij merkt de AP op dat het op voorhand kwantificeren van wat 'regelmatig' is, vaak niet goed mogelijk en/of gewenst is omdat dat afbreuk kan doen aan het vereiste niveau van bescherming in een specifieke casus. Dit zou, mede gelet op het tijdgebonden karakter van de stand van de techniek, de mogelijkheid om tijdig te kunnen inspelen op veranderde omstandigheden en toekomstige ontwikkelingen, de toepassing van de regelgeving in hoge mate kunnen belemmeren. Zo is het niet ondenkbaar dat het in de nabije toekomst mogelijk wordt om door middel van bijvoorbeeld specifieke softwaretoepassingen op eenvoudiger wijze en op grotere schaal

[42] Zie over de feitelijke bevindingen ten aanzien van de logging nader het onderzoeksrapport van de AP van maart 2019, p. 13 en 14 met daarbij de verwijzingen naar de relevante bronnen.
[43] Zie voor een toelichting op dit aantal nader bijlage(par. 2.1) bij de brief van HagaZiekenhuis van 9 augustus 2019 (kenmerk: 2019/0177/CvdW/PM/rv).
[44] Zie bijlage (par. 2.1) bij de brief van HagaZiekenhuis van 9 augustus 2019 (kenmerk: 2019/0177/CvdW/PM/rv).
[45] P. 15 (bovenaan) van het primaire besluit.
[46] Tijdens de hoorzitting (p. 6 hoorzittingsverslag) heeft HagaZiekenhuis verklaard dat er 3.500 mensen werkzaam zijn bij HagaZiekenhuis.

dossiers op logging te beoordelen. De inmiddels door HagaZiekenhuis gebruikte software [VERTROUWELIJK] ten behoeve van de controle op de logging bevestigt dit standpunt.[47]

Van professionele partijen wordt meer verwacht

62. Tot slot wordt in verband met het vorenstaande - ten overvloede - nog het volgende opgemerkt. Voor een geslaagd beroep op het lex certa-beginsel wordt van professionele partijen, zoals HagaZiekenhuis, meer verwacht dan van niet professionals. Als het gaat om professionele partijen mag worden verlangd dat zij zelf zicht hebben op de betekenis van tot hen gerichte (open) normen en zich zo nodig terdege laten informeren over de beperkingen waaraan hun gedragingen zijn onderworpen.[48] Dit klemt temeer nu het gaat om de verwerking van gegevens over gezondheid, die als gezegd kwalificeren als een bijzondere categorie van persoonsgegevens en waarvoor in beginsel een verwerkingsverbod geldt, tenzij sprake is van een uitzonderingsgrond en zorg is gedragen voor extra waarborgen. Het lag op de weg van HagaZiekenhuis, zo hierover onduidelijkheid bij haar bestond, zich zo nodig te vergewissen van de uitleg van artikel 32 AVG door middel van de in de NEN-normen vervatte tweefactor authenticatie en regelmatige controle op de logging.

63. Daarbij benadrukt de AP dat HagaZiekenhuis zelf zeer bewust was van de te nemen maatregelen op grond van artikel 32 van de AVG. Dat maakt de AP op uit de door HagaZiekenhuis zelf gemaakte beoordeling in haar autorisatiebeleid, getiteld '*Autorisatie Digitale Patiënten Dossiers*'. Hierin maakt HagaZiekenhuis uitdrukkelijk melding van de beveiligingsplicht in de AVG en wordt opgemerkt dat zorgaanbieders aan deze plicht invulling moeten geven door toepassing van de bestaande NEN normen, waaronder NEN 7510.[49]

Conclusie lex certa

64. Gelet op het vorenstaande concludeert de AP dat van een schending van het lex certa-beginsel geen sprake is. Het bezwaar dienaangaande is ongegrond.

Tweefactor authenticatie en onbevoegde toegang

65. HagaZiekenhuis stelt dat de maatregel van tweefactor authenticatie geen maatregel is die onbevoegde inzage in patiëntendossiers door medewerkers (volledig) kan voorkomen.

66. Dienaangaande merkt de AP allereerst op dat dit niet wegneemt dat deze maatregel - zoals hiervoor gemotiveerd uiteengezet - een van de verplicht te nemen passende maatregelen is in de zin van artikel 32 van de AVG en HagaZiekenhuis die maatregel dus ook moet nemen. Daarnaast merkt de AP op dat de tweefactor authenticatie een concrete (zorgspecifieke) beheersmaatregel is die, tezamen met andere beheersmaatregelen, ten doel heeft onbevoegde toegang tot systemen en toepassingen zoveel mogelijk te

[47] Zie over deze software nader de brief van HagaZiekenhuis van 24 september 20189 (kenmerk: 2018/0109x/CvdW/PM/cb) alsmede de brief van de AP van 2 december 2019.
[48] Vgl. HR, arrest van 31 oktober 2000, rov. 3.5 (ECLI:NL:HR:2000:AA7954), HR, arrest 18 januari 2005, rov. 3.4 (ECLI:NL:HR:2005:AR6579), CBb 18 december 2018, rov. 5.3.2 (ECLI:NL:CBB:2018:652).
[49] Versie 1.0, mei 2018, p. 3, onder het kopje '*c. Beveiligingsplicht'*, alsmede versie 2.0 van dat document die als bijlage 2 onderdeel uitmaakt van de *'Eindrapportage Onderzoek onrechtmatige inzage patiëntdossier'* van mei 2018 (kenmerk: 20180412ISO01).

voorkomen.[50]Dat deze maatregel, zoals HagaZiekenhuis stelt, 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. In dit kader benadrukt de AP dat het toepassen van tweefactor authenticatie - en ook de controle op de logging - niet op zichzelf staat, maar moet worden bezien in samenhang met alle andere te nemen passende maatregelen. Het is de combinatie van die maatregelen waardoor HagaZiekenhuis in staat is de bescherming van persoonsgegevens zo goed mogelijk te beheersen en inbreuken zoveel als mogelijk kan voorkomen.

Internationale waarde NEN-normen

67. HagaZiekenhuis wijst in haar bezwaarschrift nog op het in haar ogen nationale karakter van de NEN-normen. Toepassing van een nationale norm zou de uniforme toepassing van de AVG in de EU in de weg staan.

68. Ten aanzien van deze bezwaargrond merkt de AP allereerst op dat ze - zoals hiervoor onder randnummer 52 ook al is opgemerkt - gehouden is toezicht te houden op de naleving van de AVG en in dat kader in een concreet geval ook uitleg moet geven aan de in de AVG opgenomen normen, ook als het gaat om meer open normen zoals die zijn neergelegd in artikel 32 AVG. De AP heeft dat gedaan in het primaire besluit en in dit besluit via het eisen van de tweefactor authenticatie en de eis logbestanden regelmatig te beoordelen. Dat betekent niet dat daarmee (op voorhand) sprake is van een situatie die indruist tegen een autonome uitleg van de AVG. Of deze uitleg de uniforme toepassing van de AVG is de weg staat, kan desgewenst worden voorgelegd aan de nationale rechter en (uiteindelijk) aan het Europese Hof van Justitie.

Los daarvan merkt de AP nog het volgende op. De in dit geval relevante NEN-normen betreffen de Nederlandse weergave van de Europese en internationale norm NEN-ISO / IEC 27002+C1+ C2:2015 en NEN-EN-ISO 27799:2016 (en).[51] Deze normen zijn ontwikkeld in internationaal verband bij ISO(International Organization for Standardization) of IEC (International Electrotechnical Commission). ISO en IEC vormen tezamen een stelsel van organen dat gespecialiseerd is in wereldwijde normalisatie. Nationale organisaties die lid zijn van ISO of IEC participeren in het ontwikkelen van Internationale Normen via technische commissies die door de desbetreffende organisatie zijn ingesteld ten behoeve van de normalisatie in specifieke technische werkvelden. Technische commissies van ISO en IEC werken samen bij onderwerpen waarin zij een gemeenschappelijk belang hebben. Andere internationale organisaties, zowel overheidsinstanties als ngo's, nemen, in samenwerking met ISO en IEC, ook deel aan deze werkzaamheden. Op het gebied van informatietechnologie hebben ISO en IEC een gezamenlijke technische commissie opgericht, ISO/IEC JTC 1.

De documenten - en de daarin vervatte normen - die door Nederland zijn geaccepteerd, krijgen vervolgens de codering NEN-ISO of NEN-IEC. Normen met de codering: NEN-EN-ISO zijn Europees geaccepteerd.[52]

[50] Vgl. par. 9.4.1, p. 57, NEN 7510-2:2017
[51] NEN 7510-2, voorwoord, p. 7.
[52] Vgl.: https://www.nen.nl/Normontwikkeling/Wat-is-normalisatie/Europese-en-internationale-normen.htm

Kortom, het gaat bij de relevante NEN-norm dus om normen die op internationaal - en Europees niveau zijn geaccepteerd en worden gebruikt.[53]

Hoogte van de boete en dwangsom

69. Door HagaZiekenhuis worden diverse bezwaren aangevoerd die naar haar oordeel moeten leiden tot boetematiging. Die worden hierna besproken.

Nalatige verwijtbaarheid

70. HagaZiekenhuis stelt niet nalatig te zijn geweest en wijst op de door haar getroffen maatregelen.

71. Ten aanzien van deze bezwaargrond merkt de AP op dat, niettegenstaande de door HagaZiekenhuis wel getroffen maatregelen, HagaZiekenhuis ook nog andere maatregelen had moeten nemen om een passend beveiligingsniveau te waarborgen. Zoals in het primaire besluit uiteen is gezet, ziet de nalatige verwijtbaarheid op het niet hanteren van tweefactor authenticatie en het niet regelmatig controleren van de logbestanden. Die maatregelen hadden óók genomen moeten worden, en ten aanzien van die maatregelen verwijt de AP HagaZiekenhuis nalatigheid. In zoverre staan die maatregelen dus los van de door HagaZienkenhuis wel getroffen maatregelen.

72. De AP heeft gemotiveerd waarom het aantal door HagaZiekenhuis doorgevoerde steekproeven ten behoeve van de controle op de logging (evident) niet kunnen worden aangemerkt als 'regelmatige controle' en dus in strijd is met artikel 32 AVG. Dat de AP in dat verband niet op voorhand heeft aangegeven hoeveel steekproeven wél voldoende zijn, betekent nog niet dat, zoals HagaZiekenhuis betoogt, vanwege strijdigheid met de algemene beginselen van behoorlijk bestuur of het rechtszekerheidsbeginsel een bestuurlijke boete niet had kunnen worden opgelegd.[54] Ook de stelling van HagaZiekenhuis dat het handmatig controleren zeer tijdrovend is, betekent niet dat HagaZiekenhuis daarmee ontheven zou zijn van de plicht uit artikel 32 AVG en dus zou kunnen volstaan met een steekproef van zes dossiers. Bovendien wijst de AP ten aanzien van de stelling van HagaZiekenhuis dat het handmatig controleren tijdrovend is, op de mogelijkheden van specifieke softwaretoepassingen die dit in belangrijke mate kunnen ondervangen. De AP is van oordeel dat het op de weg van HagaZiekenhuis had gelegen hier eerder initiatief te tonen door hierop actief en adequaat te acteren.

Ne bis in idem

73. HagaZiekenhuis betoogt verder dat ten onrechte tweemaal een verhoging van de basisboete heeft plaatsgevonden. De onderbouwingen voor deze verhogingen komen volgens HagaZiekenhuis op hetzelfde neer. En dat is naar de mening van HagaZiekenhuis in strijd met de boetebeleidsregels van de AP en met het in artikel 5:43 Awb vervatte ne bis in idem-beginsel.

[53] De tekst van ISO/IEC 27002:2013 inclusief Cor 1:2014 en Cor 2:2015 is opgesteld door de Technische Subcommissie ISO/IEC/JTC 1/SC 27 "Information security" van de Internationale Organisatie voor Standaardisatie (ISO) en het International Elektrotechnische Comité (IEC) en is overgenomen als EN ISO/IEC 27001: 2017. (Zie het "Europees voorwoord' op p. 1 van het document NEN-EN-ISO/IEC 27002:2017).
[54] In dit verband verwijst de AP ook naar wat hierover is overwogen in randnummer 57.

74. De AP kan HagaZiekenhuis niet volgen in haar betoog en overweegt dienaangaande als volgt. De AP heeft in het primaire besluit het basisbedrag van de boete verhoogt op grond van twee factoren. Deze boete verhogende factoren staan in artikel 7, onder a en b, van de Boetebeleidsregels en zijn ontleend aan artikel 83, tweede lid, onder a en b, van de AVG.[55]

75. De eerste verhoging van de basisboete met € 75.000 op grond van de factor *'aard, ernst en duur van de inbreuk'* (artikel 7, onder a, van de Boetebeleidsregels) houdt enerzijds verband met de aard en ernst van de overtreding en anderzijds met de duur van de overtreding.
Ten aanzien van de aard/ernst is van belang dat het gaat om het ontbreken van een tweetal passende (fundamentele) beveiligingsmaatregelen, te weten een verplichte tweefactor authenticatie[56] en het regelmatig controleren en beoordelen van logbestanden. Daarnaast wordt de ernst van de overtreding nader gekleurd door het aantal medewerkers dat onbevoegd inzage heeft gehad in het desbetreffende patiëntendossier[57], het aantal patiënten dat is opgenomen in het ziekenhuisinformatiesysteem,[58] het type persoonsgegevens (gezondheidsgegevens) dat daarin is opgenomen alsmede het vertrouwen van ziekenhuispatiënten dat hierdoor in hoge mate wordt beschaamd.
Naast voormelde aard en ernst heeft ook de duur van de overtreding bijgedragen aan de (eerste) verhoging van de basisboete met € 75.000. In dat verband is van belang dat de overtreding bestond sinds in ieder geval januari 2018 en nog niet was beëindigd ten tijde van de oplegging van de boete op 18 juni 2019.

76. De tweede verhoging van de basisboete met € 75.000 is gebaseerd op artikel 7, aanhef en onder b, van de Boetebeleidsregels. Het is een verhoging vanwege de *nalatigheid* van HagaZiekenhuis. Ondanks dat de directie van HagaZiekenhuis op de hoogte was van de onbevoegde inzage van het betreffende dossier, heeft ze daarin ten onrechte geen aanleiding gezien om tijdig maatregelen te treffen die zien op een juiste implementatie van het hanteren van tweefactor authenticatie en het regelmatig controleren van de logbestanden. In dat verband merkt de AP op dat het door HagaZiekenhuis aangevoerde argument van tijdgebrek geen legitiem argument is om van het treffen van beveiligingsmaatregelen af te zien en daarmee de overtreding te laten voort bestaan.[59] Voormelde omstandigheden rechtvaardigen naar het oordeel van de AP de tweede verhoging van de basisboete met € 75.000.

77. Concluderend merkt de AP op dat de reden voor de eerste verhoging van de basisboete verschilt van die voor de tweede verhoging. De verhogingen zijn gebaseerd op verschillende factoren uit de AVG en de Boetebeleidsregels die worden meegewogen bij het vaststellen van de hoogte van de boete. Van een dubbele beboeting is dus geen sprake en het ne bis in idem-beginsel is hier dan ook niet aan de orde. Het in dat kader aangevoerde bezwaar treft geen doel.

---

[55] De is AP gehouden om met deze factoren rekening te houden bij de bepaling van de boetehoogte in een concreet geval.
[56] Het ziekenhuisinformatiesysteem heeft niet de ingebouwde verplichting, maar alleen de mogelijkheid om met tweefactor authenticatie in te loggen.
[57] Blijkens eigen onderzoek van HagaZiekenhuis *'Eindrapportage Onderzoek onrechtmatige inzage patiëntdossier'* van mei 2018, (p. 27 bovenaan) gaat het om 85 medewerkers van HagaZiekenhuis die onrechtmatig inzage hebben gehad in het patiëntdossier van de bekende Nederlander. Zie ook Onderzoeksrapport AP maart 2019, p. 4.
[58] Zoals eerder opgemerkt, gaat het in totaal om (afgerond) 381.500 patiëntbezoeken in 2017.
[59] In dit verband wijst de AP op de Richtsnoeren WP 253 waarin als voorbeeld voor de "nalatige aard van de inbreuk" wordt genoemd: het niet tijdig toepassen van technische updates (WP 253, 2016/679, p.12).

Boetematiging

78. HagaZiekenhuis is van mening dat sprake is van een boete verlagende omstandigheid als bedoeld in artikel 7, aanhef en onder c, van de Boetebeleidsregels vanwege de maatregelen die ze heeft genomen om de door betrokkenen geleden schade te beperken.

79. De AP volgt HagaZiekenhuis niet in haar betoog en overweegt als volgt. Artikel 7, aanhef en onder c, van de Boetebeleidsregels geeft de AP de mogelijkheid om de basisboete te verlagen indien er door de verwerkingsverantwoordelijke maatregelen genomen zijn om de door de betrokkenen geleden schade te beperken. De door HagaZiekenhuis getroffen maatregelen zijn erop gericht om te voldoen aan de op HagaZiekenhuis rustende verplichting ingevolge artikel 32, eerste lid, van de AVG, maar leiden er naar het oordeel van de AP niet, dan wel onvoldoende, toe dat de door de betrokkenen geleden schade is beperkt. In dat verband merkt de AP op dat HagaZiekenhhuis ten aanzien van de twee factor authenticatie en de controle op de logging zich, nadat ze naar aanleiding van het door HagaZiekenhuis zelf ingestelde onderzoek op de hoogte was van de onbevoegde inzage en vervolgens door de AP in het definitieve onderzoeksrapport van maart 2019 ook is gewezen op de geconstateerde overtredingen[60], zich onvoldoende heeft ingespannen om tijdig voldoende passende maatregelen te treffen. De AP ziet dan ook geen aanleiding tot matiging van de opgelegde boete op grond van artikel 7, aanhef en onder c, van de Boetebeleidsregels.

80. Reden voor boetematiging is er volgens HagaZiekenhuis ook omdat de boete rechtstreeks ten koste gaat van de (schaarse) middelen die anders voor patiëntenzorg hadden kunnen worden ingezet alsmede ten koste van de mogelijkheid om te investeren en te innoveren. In dit verband heeft HagaZiekenhuis ook uitdrukkelijk een beroep gedaan op verminderde draagkracht een heeft ze haar standpunt dienaangaande onderbouwd met een tweetal rapporten waarin diverse ziekenhuizen, waaronder HagaZiekenhuis, door [VERTROUWELIJK] en [VERTROUWELIJK] zijn beoordeeld op hun financiële gezondheid.[61]

81. Ook hierin ziet de AP geen reden om de boete te matigen. Bij de vaststelling van de hoogte van de bestuurlijke boete moet ingevolge artikel 5:46, tweede lid, Awb rekening worden gehouden met het evenredigheidsbeginsel. In dat verband dient het bestuursorgaan daarbij zo nodig rekening te houden met de omstandigheden waaronder de overtreding is gepleegd. Uit de parlementaire geschiedenis bij de Awb blijkt dat de draagkracht een zodanige omstandigheid kan zijn.[62] Ook in de jurisprudentie is dit bevestigd.[63]

82. Uit de jurisprudentie volgt dat als op basis van door de overtreder overgelegde financiële gegevens blijkt dat de overtreder door de boete onevenredig wordt getroffen, de boetehoogte gematigd moet worden.[64] De AP acht de financiële situatie van HagaZiekenhuis echter niet van dien aard dat daaruit moet worden

[60] P. 14-15 van het onderzoeksrapport van de AP, maart 2019.
[61] Het gaat om de rapporten [VERTROUWELIJK].
[62] Kamerstukken II, 2003/04, 29 702, P. 141.
[63] ABRvS 21 maart 2012, ECLI:NL:RVS:2012:BV9508 en HR 28 maart 2014, ECLI:NL:HR:2014:685.
[64] Zie ABRvS 12 maart 2008, ECL I:NL:RVS:2008:BV9509.

geconcludeerd dat HagaZiekenhuis onevenredig wordt getroffen door de hoogte van de boete en boetematiging vanwege verminderde draagkracht geïndiceerd is. Hierbij heeft de AP de jaarrekening van 2018 betrokken alsmede de door HagaZiekenhuis bij brief van 5 november 2019 verstrekte informatie en nadere stukken.[65]

83. Het bedrijfsresultaat van € 622.892 over het boekjaar 2018 is niet van dien aard dat HagaZiekenhuis de boete van € 460.000 niet kan dragen. Inmiddels wordt het rendement voor 2019 geprognotiseerd op € 947.000[66] Bovendien blijkt uit de jaarrekening dat HagaZiekenhuis over 2018 de beschikking had over € 24.011.362 aan vrij beschikbare liquide middelen.[67] [68] De omstandigheid dat [VERTOUWELIJK] de financiële gezondheid van HagaZiekenhuis - in het kader van een benchmark waarin ze de financiële positie van de Nederlandse algemene ziekenhuizen heeft onderzocht - heeft beoordeeld met een 4 (2017) en een 5[69] (2018) omdat haar rendement onder de 2%-norm ligt en ook onder het marktgemiddelde van 1,48%, kan HagaZiekenhuis evenmin baten. Hoewel de AP erkent dat de financiële situatie van HagaZiekenhuis slechter afsteekt ten opzichte van andere ziekenhuizen, betekent dit niet dat HagaZiekenhuis onvoldoende draagkrachtig is om de haar opgelegde boete te dragen. De AP acht de aangedragen argumentatie van HagaZiekenhuis gelet op de financiële middelen waarover ze beschikt onvoldoende om met het oog op het draagkrachtbeginsel de boete te matigen. Het zelfde geldt voor de beoordeling van [VERTROUWELIJK] die het rendement en de EBITDA[70] van Hagaziekenhuis heeft beoordeeld.

84. Dat de boete rechtstreeks ten koste gaat van de (schaarse) middelen die anders voor andere doeleinden hadden kunnen worden ingezet, onderkent de AP en ze onderschrijft de stelling van HagaZiekenhuis dat de schaarse middelen van een ziekenhuis in beginsel aan zorg dient te worden besteed. Niettemin, kan dit argument HagaZiekenhuis in dit geval niet baten. Ook het beschermen van persoonsgegevens dient op een deugdelijke wijze te zijn verankerd in de dagelijkse praktijk van een ziekenhuis waar doorlopend wordt gewerkt met bijzondere persoonsgegevens. Daarnaast zou het volgen van de lezing van HagaZiekenhuis uiteindelijk tot gevolg hebben dat een zorginstelling überhaupt niet zou kunnen worden beboet.

Last onder dwangsom

HagaZiekenhuis voldoet aan de last

[65] In dit verband merkt de AP op dat ingevolge artikel 38 UAVG de werking van de beschikking tot oplegging van een bestuurlijke boete wordt opgeschort totdat de beroepstermijn is verstreken of, indien beroep is ingesteld, totdat op het beroep is beslist. Bovendien biedt artikel 4:94 Awb de mogelijkheid een betalingsregeling te treffen.
[66] Brief HagaZiekenhuis van 5 november 2019, p. 2.
[67] Zie Jaarverslaggeving 2018 Stichting HagaZiekenhuis, 5.1 Jaarrekening, par. 5.1.5 Toelichting op de balans per 31 december 2018, p. 17.
[68] Ten overvloede wijst de AP nog op het advies uit 2016 van de voorloper van de European Data Protection Board waarbij wordt aangegeven dat verwerkingsverantwoordelijken en verwerkers inbreuken op de gegevensbeschermingswetgeving niet kunnen legitimeren door een tekort aan middelen te claimen. Zie WP 253, 2016/679, p.12.
[69] Op een schaal van 1 tot 10.
[70] EBITDA is de afkorting van Earnings Before Interest, Taxes, Depreciation and Amortization. Het wordt gebruikt als maatstaf voor de winst die een onderneming haalt met haar operationele activiteiten zonder dat hier kosten en opbrengsten van de financiering in verwerkt zitten. Zie: https://nl.wikipedia.org/wiki/EBITDA.

85. HagaZiekenhuis geeft aan haar bezwaar ten aanzien van de last onder dwangsom te handhaven, niettegenstaande de brief van de AP van 2 december 2019 waarin de AP stelt dat aan de last werd voldaan. Ze wijst er daarbij op dat de AP in die brief een voorbehoud maakt ten aanzien van de naleving van de last in de toekomst.

86. De AP merkt hierover het volgende op. In de conclusie van vorenbedoelde brief wordt aangegeven dat[71]:

> *"De AP concludeert dat ten tijde van het onderzoek ter plaatse van 17 oktober 2019 HagaZiekenhuis aan de last voldeed. Hierbij wordt wel opgemerkt dat het controleproces met [VERTROUWELIJK] dynamisch is en aan verandering onderhevig. De business rules die in combinatie met [VERTROUWELIJK] worden gebruikt, dienen continu te worden verbeterd. Deze verbetering dient onderdeel te zijn van de PDCA-verbetercyclus."*

In vorenstaand citaat is vastgelegd dat is gebleken dat HagaZiekenhuis aan de last voldeed. Op dit moment is er geen aanleiding daar anders over te oordelen. Kortom, HagaZiekenhuis voldoet aan de last. Wat de AP duidelijk heeft willen maken met voormelde passage over het controleproces met [VERTROUWELIJK], is dat de wijze waarop de verplichte controle op de logging plaats dient te vinden - als uitvloeisel van de plicht om op grond van artikel 32 AVG passende maatregelen te treffen - dynamisch van aard is. Dat houdt verband 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 (zie ook hiervoor randnummer 57). Tegen die achtergrond is HagaZienkenhuis op grond van de op haar rustende verplichting ex artikel 32 AVG gehouden om doorlopend het controleproces te monitoren en zo nodig te verbeteren, specifiek waar het gaat om het verfijnen van de business rules. Dat staat los van de constatering dat HagaZiekenhuis op dit moment aan de last voldoet. Wat nu echter als passend wordt beschouwd, hoeft dat in de (nabije) toekomst niet meer te zijn. Het is ook om die reden dat wordt verlangd dat verwerkingsverantwoordelijken de PDCA-verbetercyclus doorlopen om zo - ter naleving van artikel 32 AVG en destijds artikel 13 Wbp - een blijvend passend beveiligingsniveau in de organisatie te waarborgen.[72] Dat is wat de AP in haar brief van 2 december 2019 aan HagaZiekenhuis heeft willen meegeven, maar dat doet dus niet af aan de omstandigheid dat de AP van oordeel is dat HagaZiekenhuis voldoet aan de last. Wel is het zo dat, zoals de AP ook in haar brief van 2 december 2019 heeft aangegeven, de last onder dwangsom niet is opgeheven en in de (nabije) toekomst opnieuw kan onderzoeken of de last nog steeds wordt nageleefd. Dat volgt uit artikel 5:34, tweede lid, van de, Awb.[73]

Hoogte dwangsom; gelijkheidsbeginsel en evenredigheid

87. HagaZiekenhuis stelt zich verder op het standpunt dat de hoogte van de dwangsommen niet in verhouding staan tot de verweten gedraging. Daarmee is het bestreden besluit volgens HagaZiekenhuis in strijd met het evenredigheidsbeginsel in de zin van artikel 3:4 Awb en eveneens met de specifieke bepaling in artikel

[71] Brief AP d.d. 2 december 2019, p. 8.
[72] In haar richtsnoeren van februari 2013 heeft het CBb destijds uitleg gegeven aan wat passende maatregelen inhouden. Deze richtsnoeren zijn wat dat betreft nog steeds actueel en bruikbaar. Zie: https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-publiceert-richtsnoeren-beveiliging-van-persoonsgegevens
[73] Opheffing is in onderhavig geval pas aan de orde als HagaZiekenhuis daartoe op grond van artikel 5:34 Awb een verzoek doet.

5:32b, lid 3 Awb. Naar het oordeel van de AP wordt deze bezwaargrond tevergeefs aangevoerd en overweegt dienaangaande als volgt.

88. Vooropgesteld zij dat HagaZiekenhuis heeft voldaan aan de last en er geen dwangsommen zijn verbeurd. De AP ziet om die reden niet in welk belang HagaZiekenhis nog heeft bij de aangevoerde bezwaargronden ten aanzien van de last onder dwangsom. Los daarvan, merkt de AP het volgende op.

89. De hoogte van de dwangsom dient in een redelijke verhouding te staan tot enerzijds de zwaarte van het door de overtreding van het wettelijke voorschrift geschonden belang en anderzijds de beoogde effectieve werking van de dwangsomoplegging. Daarbij is van belang dat van de dwangsom een zodanige prikkel moet uitgaan, dat de opgelegde last wordt nagekomen en verbeurte van de dwangsom wordt voorkomen. De AP is van oordeel dat in dit geval een dwangsom is opgelegd waarbij sprake is van een redelijke verhouding in vorenbedoelde zin en overweegt als volgt.

90. Ten aanzien van de zwaarte van het door de overtreding van het wettelijke voorschrift geschonden belang benadrukt de AP dat het gaat om uiterst gevoelige gegevens over gezondheid. Deze gegevens kwalificeren, zoals meermaals opgemerkt, als een bijzondere categorie van persoonsgegevens in de zin van artikel 9, eerste lid, AVG waarvoor in beginsel een verwerkingsverbod geldt tenzij sprake is van een uitzondering als vermeld in de AVG en UAVG. Voor het vertrouwen van patiënten in een zorgverlener is het van groot belang dat met deze persoonsgegevens uiterst zorgvuldig wordt omgegaan en dat ze qua beveiliging voldoen aan de hoogste normen. In dat kader wordt opgemerkt dat het in casu gaat om het ontbreken van een tweetal fundamentele beveiligingsmaatregelen en dat, ondanks dat de directie van HagaZiekenhuis op de hoogte was van de onbevoegde inzage van het betreffende dossier, daarin ten onrechte geen aanleiding heeft gezien om tijdig maatregelen te treffen die zien op een juiste implementatie van het hanteren van tweefactor authenticatie en het regelmatig controleren van de logbestanden. Deze omstandigheden rechtvaardigen daarom naar het oordeel van de AP de hoogte van de dwangsom zoals die in het bestreden besluit zijn vastgesteld.

91. HagaZiekenhuis is van mening dat de vastgestelde dwangsom in strijd is met het gelijkheidsbeginsel en wijst daarbij op eerder door de AP opgelegde lasten waarbij lagere dwangsommen zijn vastgesteld. Deze bezwaargrond treft naar het oordeel van de AP geen doel en licht dat standpunt als volgt toe.

92. In algemene zin zij opgemerkt dat de enkele omstandigheid dat de dwangsom in het geval van HagaZiekenhuis de hoogste zou zijn in vergelijking met dwangsommen die de AP eerder heeft opgelegd, niet betekent dat de dwangsom in dit geval dus te hoog is of in strijd met het gelijkheidsbeginsel. De hoogte van een dwangsom wordt casus specifiek beoordeeld en vastgesteld waarbij acht wordt geslagen op alle relevante omstandigheden van het concrete geval.

93. Ten aanzien van de dwangsommen die in 2009 aan andere zorgverleners zijn opgelegd[74], en waaraan HagaZiekenhuis met een beroep op het gelijkheidsbeginsel refereert, merkt de AP op dat dat gevallen betrof uit een betrekkelijk ver verleden (inmiddels tien jaar geleden) - ze vonden plaats in een andere

[74] Het ging in die zaken op dwangsommen van€ 1.000 en €2.000 per dag met maxima van €30.000 en € 60.000.

tijdsgeest en dateren van vóór de AVG - en waarbij sprake was van overtredingen van een duidelijk andere aard. Het betrof het niet voldoen aan verplichtingen met een (voornamelijk) administratief karakter, zoals het niet uitvoeren van een risicoanalyse, het niet opstellen van een rapportage van de risicoanalyse informatiebeveiliging dan wel een functieprofiel informatiebeveiligingsfunctionaris, het niet aanstellen/aanwijzen van een informatiebeveiligingsfunctionaris en een portefeuillehouder informatiebeveiliging. In geval van HagaZiekenhuis gaat om twee fundamentele beveiligingsmaatregelen - tweefactor authenticatie en regelmatige logging - die niet zijn toegepast. Bovendien ging er ingeval van HagaZiekenhuis een ernstig beveiligingsincident aan vooraf, waarmee ook de context duidelijk anders was. Evenzeer is in dit verband nog van belang op te merken dat het CBP - de voorloper van de AP - al eerder in 2013 na onderzoek bij diverse zorginstellingen heeft geconstateerd dat niet werd voorzien in voldoende passende maatregelen ten aanzien van toegang tot patiëntendossiers (behandelrelatie) en ten aanzien van de controle op de logging.[75]

94. Waar het gaat om de dwangsom in de zaak van de Nationale Politie, en waarbij HagaZieknhuis erop wijst dat het in die zaak om dwangsom ging van € 50.000 per twee weken, merkt de AP op dat het in dat geval één overtreding betrof en geen twee zoals in onderhavige casus. Deze omstandigheid maakt het verschil in de opgelegde dwangsommen naar het oordeel van de AP verklaarbaar. Bovendien is het maximumbedrag van € 320.000 ingeval van de Nationale Politie vergelijkbaar. Tot slot zij opgemerkt dat zich in de casus van HagaZiekenhuis daadwerkelijk een ernstig beveiligingsincident heeft voorgedaan.

95. In aanvulling op het vorenstaande en ter illustratie van het casus specifieke karakter van de hoogte van een dwangsom wijst de AP nog op de in 2018 aan VGZ opgelegde last onder dwangsom. De hoogte van de dwangsom bedroeg daar € 150.000 per week en met een maximum van € 750.000, vanwege een feit dat medewerkers van VGZ feitelijk toegang hadden tot persoonsgegevens betreffende de gezondheid terwijl dat voor hun werkzaamheden niet noodzakelijk was (zonder dat overigens was vastgesteld dat deze medewerkers daadwerkelijk deze gegevens hebben geraadpleegd).[76] Hieruit volgt dat de AP ook hogere dwangsommen oplegt in een casus die op belangrijke punten vergelijkbaar is met onderhavige last onder dwangsom.

96. Volgens HagaZiekenhuis is de vastgestelde dwangsom verder nog in strijd met het evenredigheidsbeginsel omdat één dwangsombedrag is verbonden aan een last die uit twee onderdelen bestaat waardoor ook dwangsommen worden verbeurd als het eerste onderdeel van de last wel, maar het tweede onderdeel van de last niet wordt uitgevoerd. De AP kan het standpunt van HagaZiekenhuis niet volgen en merkt het volgende op.

97. Op zichzelf bestaat er geen plicht om de last onder dwangsom op de door HagaZiekenhuis voorgestelde wijze te splitsen, en daar is volgens de AP in dit geval ook geen aanleiding voor. De aan HagaZiekenhuis opgelegde last betreft het uitvoeren van twee maatregelen die beiden verband houden met de naleving van de verplichting om ingevolge artikel 32 AVG passende beveiligingsmaatregelen te nemen. Aan beide

[75] https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/rap_2013-patientendossiers-binnen-zorginstellingen.pdf
[76] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_last_onder_dwangsom_vgz.pdf

verplichtingen moet worden voldaan om te bewerkstellingen dat artikel 232 AVG wordt nageleefd. Het gaat om een cumulatie van maatregelen die er te samen voor zorgt dat in overeenstemming met artikel 32 AVG wordt gehandeld. Ook als aan één van deze verplichtingen niet wordt voldaan, is dus nog steeds sprake van schending van artikel 32 AVG. Het gaat erom dat wordt bewerkstelligd dat gelijktijdig wordt voldaan aan alle verplichtingen die volgen uit de plicht om passende maatregelen te nemen.

98. HagaZiekenhuis wijst ten slotte nog op de enorme uitdaging van HagaZiekenhuis om financieel gezond te blijven en betoogt dat de last onder dwangsom ten koste gaat van de mogelijkheid om te investeren en te innoveren in de zorg. Dat kan volgens HagaZiekenhuis niet de bedoeling zijn van handhaving en dat rechtvaardigt volgens HagaZiekenhuis een verlaging van de dwangsom. De AP volgt het betoog van HagaZiekenhuis niet en overweegt als volgt.

99. Van de last onder dwangsom moet een zodanige prikkel uitgaan, dat de opgelegde last wordt uitgevoerd zonder dat een dwangsom wordt verbeurd.[77] Met dit standpunt verhoudt zich niet dat bij het bepalen van de dwangsom rekening wordt gehouden met de omstandigheid dat het verbeuren van de dwangsom ten koste gaat van de mogelijkheid om te investeren en te innoveren in de zorg omdat dan de prikkel om de last uit te voeren te zeer wordt weggenomen. In dit verband trekt de AP de vergelijking met de uitspraak van de Afdeling bestuursrechtspraak van de Raad van State van 6 februari 2019[78] waaruit volgt dat een dwangsom die naar draagkracht zou worden bepaald, onvoldoende prikkel geeft aan de overtreder om de last te beëindigen. Ook uit eerdere jurisprudentie volgt dat de financiële omstandigheden van de overtreder in beginsel geen rol (mogen) spelen bij het vaststellen van de hoogte van de dwangsom.[79] De AP beschouwt de door HagaZiekenhuis in dit verband aangevoerde bezwaargrond ook als een beroep op zodanige financiële omstandigheden en is van oordeel dat die in dit geval geen rol mogen spelen bij de vaststelling van de hoogte van de dwangsom.

Conclusie

100. Ingevolge artikel 7:11, eerste lid, van de Algemene wet bestuursrecht heeft de AP het bestreden besluit heroverwogen naar aanleiding van de aangevoerde bezwaren. Bij deze heroverweging heeft de AP beoordeeld of zij terecht heeft besloten tot het opleggen van een boete en last onder dwangsom.

101. Gelet op het voorgaande is de AP van oordeel dat zij bij het nemen van het primaire besluit terecht tot de oplegging van de boete en last onder dwangsom is overgegaan. Ook is er geen sprake van een verandering van relevante feiten en omstandigheden sinds het primaire besluit, zodat er geen aanleiding bestaat het primaire besluit te herroepen en een andersluidend besluit te nemen.

[77] Zie bijv. ABRvS 10 juli 2019 (ECLI:NL:RVS:2019:2343), ABRvS 12 juni 2019 (ECLI:NL:RVS:2019:1870) en ABRvS 17 april 2019 (ECLI:NL:RVS:2019:1243).
[78] ECLI:NL:RVS:2019:321.
[79] ABRvS 26 oktober 2016 (ECLI:NL:RVS:2016:2797).

Datum
15 januari 2020

Ons kenmerk
z2019-17017

Datum
15 januari 2020

Ons kenmerk
z2019-17017

7. Dictum

De Autoriteit Persoonsgegevens verklaart het bezwaar ongegrond.

Hoogachtend,
Autoriteit Persoonsgegevens,

mr. A. Wolfsen
Voorzitter

Rechtsmiddelenclausule

Indien u het niet eens bent met dit besluit kunt u binnen zes weken na de datum van verzending van het besluit ingevolge de Algemene wet bestuursrecht een beroepschrift indienen bij de rechtbank (sector bestuursrecht) in het arrondissement, waarbinnen uw woonplaats valt. U dient een afschrift van dit besluit mee te zenden.

Datum
15 januari 2020

Ons kenmerk
z2019-17017

BIJLAGE

Juridisch kader

Algemeen

De AP beoordeelt ingevolge artikel 7:11 van de Algemene wet bestuursrecht (Awb) op grond van uw bezwaar of zij bij het primaire besluit terecht heeft besloten tot afwijzing van uw AVG-klacht. De heroverweging geschiedt (in beginsel) met inachtneming van alle feiten en omstandigheden zoals die zijn op het tijdstip van de heroverweging.

AVG

Artikel 32 Beveiliging van de verwerking
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's 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) 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.

4. De verwerkingsverantwoordelijke en de verwerker treffen maatregelen om ervoor te zorgen dat iedere natuurlijke persoon die handelt onder het gezag van de verwerkingsverantwoordelijke of van de verwerker en toegang heeft tot persoonsgegevens, deze slechts in opdracht van de verwerkingsverantwoordelijke verwerkt, tenzij hij daartoe Unierechtelijk of lidstaatrechtelijk is gehouden.

Datum
15 januari 2020

Ons kenmerk
z2019-17017

Artikel 58 Bevoegdheden

1. Elk toezichthoudende autoriteit heeft alle volgende onderzoeksbevoegdheden om:

a) de verwerkingsverantwoordelijke, de verwerker en, in voorkomend geval, de vertegenwoordiger van de verwerkingsverantwoordelijke of van verwerker te gelasten alle voor de uitvoering van haar taken vereiste informatie te verstrekken;

b) onderzoeken te verrichten in de vorm van gegevensbeschermingscontroles;

c) een toetsing te verrichten van de overeenkomstig artikel 42, lid 7, afgegeven certificeringen;

d) de verwerkingsverantwoordelijke of de verwerker in kennis te stellen van een beweerde inbreuk op deze verordening;

e) van de verwerkingsverantwoordelijke en de verwerker toegang te verkrijgen tot alle persoonsgegevens en alle informatie die noodzakelijk is voor de uitvoering van haar taken; en

f) toegang te verkrijgen tot alle bedrijfsruimten van de verwerkingsverantwoordelijke en de verwerker, daaronder begrepen tot alle uitrustingen en middelen voor gegevensverwerking, in overeenstemming met het uniale of lidstatelijke procesrecht.

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

a) de verwerkingsverantwoordelijke of de verwerker waarschuwen dat met de voorgenomen verwerkingen waarschijnlijk inbreuk op bepalingen van deze verordening wordt gemaakt;

b) de verwerkingsverantwoordelijke of de verwerker berispen wanneer met verwerkingen inbreuk op bepalingen van deze verordening is gemaakt;

c) de verwerkingsverantwoordelijke of de verwerker gelasten de verzoeken van de betrokkene tot uitoefening van zijn rechten uit hoofde van deze verordening in te willigen;

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;

e) de verwerkingsverantwoordelijke gelasten een inbreuk in verband met persoonsgegevens aan de betrokkene mee te delen;

f) een tijdelijke of definitieve verwerkingsbeperking, waaronder een verwerkingsverbod, opleggen;

g) het rectificeren of wissen van persoonsgegevens of het beperken van verwerking uit hoofde van de artikelen 16, 17 en 18 gelasten, alsmede de kennisgeving van dergelijke handelingen aan ontvangers aan wie de persoonsgegevens zijn verstrekt, overeenkomstig artikel 17, lid 2, en artikel 19;

h) een certificering intrekken of het certificeringsorgaan gelasten een uit hoofde van de artikelen 42 en 43 afgegeven certificering in te trekken, of het certificeringsorgaan te gelasten geen certificering af te geven indien niet langer aan de certificeringsvereisten wordt voldaan;

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

j) de opschorting van gegevensstromen naar een ontvanger in een derde land of naar een internationale organisatie gelasten.

3. Elke toezichthoudende autoriteit heeft alle autorisatie- en adviesbevoegdheden om:

a) de verwerkingsverantwoordelijke advies te verstrekken in overeenstemming met de procedure van voorafgaande raadpleging van artikel 36;
b) op eigen initiatief dan wel op verzoek, aan het nationaal parlement, aan de regering van de lidstaat, of overeenkomstig het lidstatelijke recht aan andere instellingen en organen alsmede aan het publiek advies te verstrekken over aangelegenheden die verband houden met de bescherming van persoonsgegevens;
c) toestemming te geven voor verwerking als bedoeld in artikel 36, lid 5, indien die voorafgaande toestemming door het lidstatelijke recht wordt voorgeschreven;
d) overeenkomstig artikel 40, lid 5, advies uit te brengen over en goedkeuring te hechten aan de ontwerpgedragscodes;
e) certificeringsorganen te accrediteren overeenkomstig artikel 43;
f) certificeringen af te geven en certificeringscriteria goed te keuren overeenkomstig artikel 42, lid 5;
g) de in artikel 28, lid 8, en artikel 46, lid 2, punt d), bedoelde standaardbepalingen inzake gegevensbescherming aan te nemen;
h) toestemming te verlenen voor de in artikel 46, lid 3, punt a), bedoelde contractbepalingen;
i) toestemming te verlenen voor de in artikel 46, lid 3, punt b), bedoelde administratieve regelingen;
j) goedkeuring te hechten aan bindende bedrijfsvoorschriften overeenkomstig artikel 47.

4. Op de uitoefening van de bevoegdheden die uit hoofde van dit artikel aan de toezichthoudende autoriteit worden verleend, zijn passende waarborgen van toepassing, daaronder begrepen doeltreffende voorziening in rechte en eerlijke rechtsbedeling, zoals overeenkomstig het Handvest vastgelegd in het Unierecht en het lidstatelijke recht.

5. Elke lidstaat bepaalt bij wet dat zijn toezichthoudende autoriteit bevoegd is inbreuken op deze verordening ter kennis te brengen van de gerechtelijke autoriteiten en, waar passend, daartegen een rechtsvordering in te stellen of anderszins in rechte op te treden, teneinde de bepalingen van deze verordening te doen naleven.

6. Elke lidstaat kan bij wet bepalen dat zijn toezichthoudende autoriteit, naast de in lid 1, 2 en 3 bedoelde bevoegdheden bijkomende bevoegdheden heeft. De uitoefening van die bevoegdheden doet geen afbreuk aan de doeltreffende werking van hoofdstuk VII.

Artikel 83 Algemene voorwaarden voor het opleggen van administratieve geldboeten

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. Bij het besluit over de vraag of een administratieve geldboete wordt opgelegd en over de hoogte daarvan wordt voor elk concreet geval naar behoren rekening gehouden met het volgende:

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;
d) de mate waarin de verwerkingsverantwoordelijke of de verwerker verantwoordelijk is gezien de technische en organisatorische maatregelen die hij heeft uitgevoerd overeenkomstig de artikelen 25 en 32;
e) eerdere relevante inbreuken door de verwerkingsverantwoordelijke of de verwerker;
f) de mate waarin er met de toezichthoudende autoriteit is samengewerkt om de inbreuk te verhelpen en de mogelijke negatieve gevolgen daarvan te beperken;
g) de categorieën van persoonsgegevens waarop de inbreuk betrekking heeft;
h) de wijze waarop de toezichthoudende autoriteit kennis heeft gekregen van de inbreuk, met name of, en zo ja in hoeverre, de verwerkingsverantwoordelijke of de verwerker de inbreuk heeft gemeld;
i) de naleving van de in artikel 58, lid 2, genoemde maatregelen, voor zover die eerder ten aanzien van de verwerkingsverantwoordelijke of de verwerker in kwestie met betrekking tot dezelfde aangelegenheid zijn genomen;
j) het aansluiten bij goedgekeurde gedragscodes overeenkomstig artikel 40 of van goedgekeurde certificeringsmechanismen overeenkomstig artikel 42; en
k) elke andere op de omstandigheden van de zaak toepasselijke verzwarende of verzachtende factor, zoals gemaakte financiële winsten, of vermeden verliezen, die al dan niet rechtstreeks uit de inbreuk voortvloeien.

3. Indien een verwerkingsverantwoordelijke of een verwerker opzettelijk of uit nalatigheid met betrekking tot dezelfde of daarmee verband houdende verwerkingsactiviteiten een inbreuk pleegt op meerdere bepalingen van deze verordening, is de totale geldboete niet hoger dan die voor de zwaarste inbreuk.

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) de verplichtingen van de verwerkingsverantwoordelijke en de verwerker overeenkomstig de artikelen 8, 11, 25 tot en met 39, en 42 en 43;
b) de verplichtingen van het certificeringsorgaan overeenkomstig de artikelen 42 en 43;
c) de verplichtingen van het toezichthoudend orgaan overeenkomstig artikel 41, lid 4.

5. Inbreuken op onderstaande bepalingen zijn overeenkomstig lid 2 onderworpen aan administratieve geldboeten tot 20 000 000 EUR of, voor een onderneming, tot 4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is:

a) de basisbeginselen inzake verwerking, met inbegrip van de voorwaarden voor toestemming, overeenkomstig de artikelen 5, 6, 7 en 9;
b) de rechten van de betrokkenen overeenkomstig de artikelen 12 tot en met 22;
c) de doorgiften van persoonsgegevens aan een ontvanger in een derde land of een internationale organisatie overeenkomstig de artikelen 44 tot en met 49;
d) alle verplichtingen uit hoofde van krachtens hoofdstuk IX door de lidstaten vastgesteldrecht;
e) niet-naleving van een bevel of een tijdelijke of definitieve verwerkingsbeperking of een opschorting van gegevensstromen door de toezichthoudende autoriteit overeenkomstig artikel 58, lid 2, of niet-verlening van toegang in strijd met artikel 58, lid 1.

6. Niet-naleving van een bevel van de toezichthoudende autoriteit als bedoeld in artikel 58, lid 2, is overeenkomstig lid 2 van dit artikel onderworpen aan administratieve geldboeten tot 20 000 000 EUR of, voor een onderneming, tot 4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is.

7. Onverminderd de bevoegdheden tot het nemen van corrigerende maatregelen van de toezichthoudende autoriteiten overeenkomstig artikel 58, lid 2, kan elke lidstaat regels vaststellen betreffende de vraag of en in hoeverre administratieve geldboeten kunnen worden opgelegd aan in die lidstaat gevestigde overheidsinstanties en overheidsorganen.

8. De uitoefening door de toezichthoudende autoriteit van haar bevoegdheden uit hoofde van dit artikel is onderworpen aan passende procedurele waarborgen overeenkomstig het Unierecht en het lidstatelijke recht, waaronder een doeltreffende voorziening in rechte en eerlijke rechtsbedeling.

9. Wanneer het rechtsstelsel van de lidstaat niet voorziet in administratieve geldboeten, kan dit artikel aldus worden toegepast dat geldboeten worden geïnitieerd door de bevoegde toezichthoudende autoriteit en opgelegd door bevoegde nationale gerechten, waarbij wordt gewaarborgd dat deze rechtsmiddelen doeltreffend zijn en eenzelfde effect hebben als de door toezichthoudende autoriteiten opgelegde administratieve geldboeten. De boeten zijn in elk geval doeltreffend, evenredig en afschrikkend. Die lidstaten delen de Commissie uiterlijk op 25 mei 2018 de wetgevingsbepalingen mee die zij op grond van dit lid vaststellen, alsmede onverwijld alle latere wijzigingen daarvan en alle daarop van invloed zijnde wijzigingswetgeving.

UAVG

Artikel 14 Taken en bevoegdheden
1. De Autoriteit persoonsgegevens is bevoegd om de taken uit te voeren en de bevoegdheden uit te oefenen die bij of krachtens de verordening zijn toegekend aan de toezichthoudende autoriteit.

2. Op de voorbereiding van een besluit omtrent goedkeuring van een gedragscode, dan wel de wijziging of uitbreiding daarvan, als bedoeld in artikel 40, vijfde lid, van de verordening is afdeling 3.4 van de Algemene wet bestuursrecht van toepassing.

3. 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.

4. De artikelen 5:4 tot en met 5:10a de Algemene wet bestuursrecht zijn van overeenkomstige toepassing op corrigerende maatregelen als bedoeld in artikel 58, tweede lid, onderdelen b tot en met j van de verordening.

5. Onverminderd artikel 4:15 van de Algemene wet bestuursrecht kan de Autoriteit Persoonsgegevens de termijn voor het geven van een beschikking opschorten voor zover dit noodzakelijk is in verband met het naleven van op de Autoriteit Persoonsgegevens rustende verplichtingen op grond van de artikelen 60 tot en met 66 van de verordening. Het derde en vierde lid van artikel 4:15 van de Algemene wet bestuursrecht zijn op deze opschorting van overeenkomstige toepassing.