AUTORITEIT
PERSOONSGEGEVENS

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

Vertrouwelijk/Aangetekend
[VERTROUWELIJK]

Datum
4 februari 2021

Ons kenmerk
[vertrouwelijk]

Contactpersoon
[vertrouwelijk]

Onderwerp
Besluit tot het opleggen van een bestuurlijke boete

Geachte [betrokkene],

De Autoriteit Persoonsgegevens (hierna: AP) heeft besloten om u een **bestuurlijke boete** van **€ 12.000,00** op te leggen. De AP is van oordeel dat u in ieder geval in de periode van 1 juli 2018 tot en met 29 mei 2019 niet heeft voldaan aan uw verplichting om bij het verwerken van persoonsgegevens passende technische en organisatorische maatregelen te treffen (artikel 32, eerste lid, van de Algemene verordening gegevensbescherming; hierna: AVG).

Hierna wordt het besluit toegelicht. Paragraaf 1 bevat een inleiding. In paragraaf 2 wordt ingegaan op de verwerking, verwerkingsverantwoordelijkheid en de geconstateerde overtreding. In paragraaf 3 wordt ingegaan op de bevoegdheid van de AP om een boete op te leggen, en de hoogte van de boete. Paragraaf 4 bevat tot slot de beslissing (het dictum) en de rechtsmiddelenclausule.

1. Inleiding

1.1. Over de overtreder

De onderneming "[onderneming]" wordt gedreven door [betrokkene]. Op de website van de orthodontiepraktijk is vermeld dat de praktijk, naast [betrokkene] als orthodontist, elf werknemers heeft. De praktijk is gevestigd aan de [adres] en de onderneming is ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer [kvk-nummer].

1.2. Aanleiding voor het onderzoek en procesverloop

Op 27 november 2018 heeft de AP een klacht ontvangen als bedoeld in artikel 77 van de AVG. Volgens de klacht worden via het inschrijfformulier op de website van de orthodontiepraktijk gevoelige gegevens gevraagd, zoals het burgerservicenummer (hierna: BSN), maar worden de gegevens vervolgens niet-versleuteld verzonden.

De AP heeft op 26 februari 2019 de website van de orthodontiepraktijk bezocht en daarvan screenshots gemaakt.

Bij brief van 29 mei 2019 heeft de AP [betrokkene] om inlichtingen verzocht. [Betrokkene] heeft daar bij brief van 4 juni 2019 op gereageerd.

De AP heeft op 4 juli 2019 opnieuw de website van de orthodontiepraktijk bezocht en daarvan screenshots gemaakt.

Bij brief van 12 augustus 2019 heeft de AP [betrokkene] om nadere inlichtingen verzocht. [Betrokkene] heeft daar bij brief van 19 augustus 2019 op gereageerd.

De bevindingen en conclusies van het onderzoek zijn vastgelegd in een rapport van 27 augustus 2019.

Bij brief van 12 september 2019 heeft de AP het onderzoeksrapport aan [betrokkene] gezonden. De AP heeft daarbij het voornemen geuit om een bestuurlijke boete op te leggen en [betrokkene] in de gelegenheid gesteld om daarop een zienswijze te geven.

Bij brief van 7 oktober 2019, aangevuld bij die van 9 en 12 december 2019, heeft [betrokkene] een zienswijze ingediend.

2. Feiten en beoordeling

De relevante wet- en regelgeving is vermeld in de bijlage bij dit besluit.

2.1. Verwerking van persoonsgegevens

Ten tijde van de klacht bevatte de website van de orthodontiepraktijk een formulier voor het inschrijven van nieuwe patiënten. Dit formulier bevatte velden voor onder meer NAW-gegevens, geboortedatum, BSN, telefoonnummers van de patiënt en de ouders, gegevens over de school, huisarts, tandarts en de verzekeringsmaatschappij. Deze gegevens betreffen informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, en zijn aldus persoonsgegevens als bedoeld in artikel 4, aanhef en onder 1, van de AVG.

Uit de brief van [betrokkene] van 19 augustus 2019 volgt dat na het verzenden van het formulier, de ingevulde gegevens online werden opgeslagen. De orthodontiepraktijk ontving per e-mail een melding van de nieuwe inschrijving. Een medewerker van de praktijk logde in op de website, opende de gegevens van de inschrijving en maakte een nieuwe patiënt aan in het eigen patiëntenbestand. Vervolgens werden de online opgeslagen gegevens verwijderd, aldus [betrokkene]. Dit geheel van verwerkingen, maar ook ieder onderdeel daarvan, waaronder het vastleggen, opslaan en vernietigen van gegevens, is een verwerking van persoonsgegevens als bedoeld in artikel 4, aanhef en onder 2, van de AVG.

2.2. Verwerkingsverantwoordelijke

[Betrokkene] bepaalt het doel en de middelen van de verwerking van persoonsgegevens. Het inschrijfformulier dient er immers toe om gegevens te verkrijgen van nieuwe patiënten van de door haar als eenmanszaak gevoerde orthodontiepraktijk, benodigd voor de behandeling en de financiële afhandeling daarvan. [Betrokkene] is aldus de verwerkingsverantwoordelijke, bedoeld in artikel 4, aanhef en onder 7, van de AVG.

2.3. Overtreding met betrekking tot de beveiliging van de verwerking

2.3.1. Inleiding

De verwerkingsverantwoordelijke is er op grond van artikel 32, eerste lid, van de AVG toe gehouden om passende technische en organisatorische maatregelen te treffen, om de verwerking van persoonsgegevens te beveiligen tegen onder meer verlies of onrechtmatige verwerking van de gegevens. Deze maatregelen dienen een passend beveiligingsniveau te waarborgen, rekening houdend met de stand van de techniek en de uitvoeringskosten, de risico's van de verwerking en de aard van de te beschermen gegevens.

De vraag of de verwerkingsverantwoordelijke de in artikel 32, eerste lid, van de AVG genoemde maatregelen heeft getroffen, wordt in gevallen als het voorliggende als volgt beoordeeld. De verwerking van het BSN van een patiënt door een zorgverlener dient te voldoen aan NEN 7510. Dat is een informatiebeveiligingsnorm voor de gezondheidszorg. De verplichting om aan die norm te voldoen volgt uit artikel 2 van de Regeling gebruik burgerservicenummer in de zorg, gelezen in samenhang met artikel 8 van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg.[1] Ook buiten deze wettelijke plicht met betrekking tot het BSN, geldt voor de gezondheidszorg dat NEN 7510 de algemeen geaccepteerde beveiligingsstandaarden bevat.[2] NEN 7510 is nader uitgewerkt in NEN 7510-1 en NEN 7510-2.

In hoofdstuk 10 van NEN 7510-2 wordt ingegaan op beheersmaatregelen met betrekking tot cryptografie. Deze maatregelen hebben ten doel te zorgen voor correct en doeltreffend gebruik van cryptografie om de

[1] Artikel 8, eerste lid, van deze wet heeft betrekking op het verlenen van zorg. Uit artikel 1, aanhef en onder b, van die wet volgt dat de financieel-administratieve afwikkeling daar ook toe behoort. Die afwikkeling begint met het doen aanleveren van de daarvoor vereiste gegevens, zoals het BSN. Vergelijk de totstandkomingsgeschiedenis van deze bepaling (Kamerstukken II 2005/06, 30 380, nr. 3, blz. 20).
[2] Vergelijk de CBP Richtsnoeren Beveiliging van persoonsgegevens (Stcrt. 2013 nr. 5174, p. 11).

vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen. In paragraaf 10.1.1 is vermeld dat ter bescherming van informatie een beleid voor het gebruik van cryptografische beheersmaatregelen behoort te worden ontwikkeld en geïmplementeerd. Deze kunnen onder meer worden gebruikt met het doel de vertrouwelijkheid te waarborgen, door de codering van informatie te gebruiken om gevoelige of essentiële informatie, tijdens opslag of verzending, te beschermen.

In hoofdstuk 13 van NEN 7510-2 wordt ingegaan op beheersmaatregelen met betrekking tot communicatiebeveiliging. Paragraaf 13.2 bevat beheersmaatregelen met betrekking tot informatietransport. Het doel van deze beheersmaatregelen is het handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit. In paragraaf 13.2.1 is vermeld dat bij het gebruik van communicatiefaciliteiten voor informatietransport, in overweging moet worden genomen gebruik te maken van cryptografische technieken, bijvoorbeeld om de vertrouwelijkheid, integriteit en authenticiteit van informatie te beschermen.

Met betrekking tot de stand van de techniek ten aanzien van cryptografische technieken is verder van belang dat ook het Nationaal Cyber Security Centrum (hierna: NCSC) op diens website wijst op het belang van het beschermen van communicatie als gevoelige informatie via een verbinding wordt verstuurd.[3] Volgens het NCSC is TLS (Transport Layer Security) het meest gebruikte protocol voor het beveiligen van verbindingen op internet. Toepassing van TLS op webverkeer geschiedt via het HTTPS-protocol aan de hand van een TLS-certificaat.

Een TLS-certificaat kan kosteloos worden verkregen,[4] al dienen in de regel kosten te worden gemaakt om het certificaat door een IT'er op de server te laten installeren of vernieuwen omdat de geldigheidsduur is verstreken. Dit zijn kortdurende handelingen waar slechts loonkosten mee gemoeid zijn.

2.3.2. Feiten

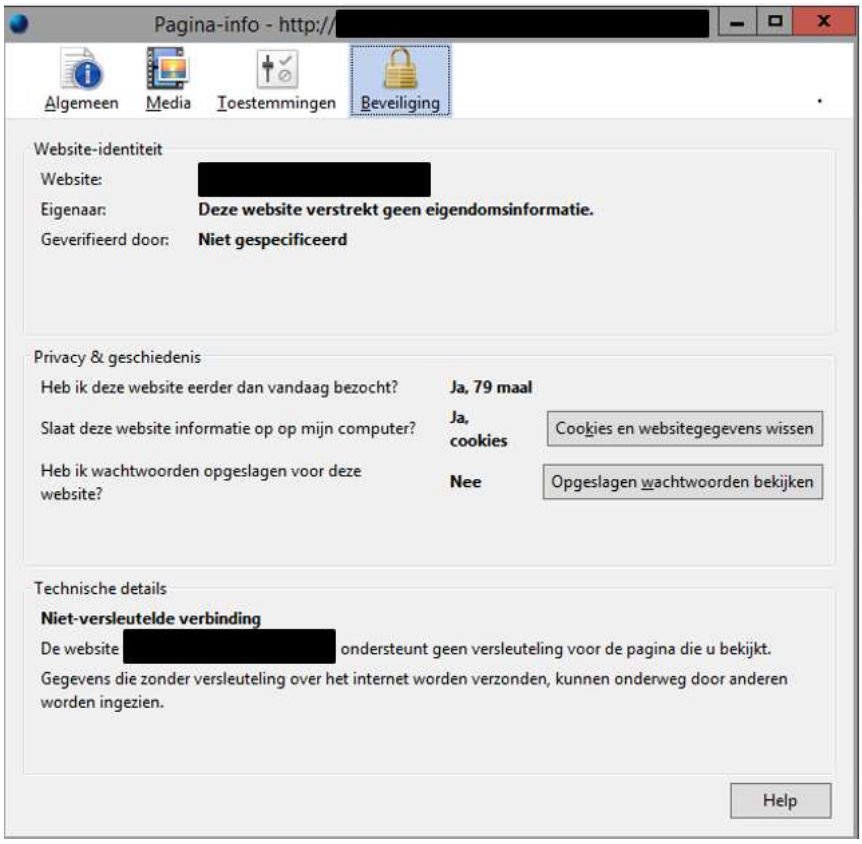
[Betrokkene] heeft verklaard dat de website van de orthodontiepraktijk op 4 juni 2010 online is gegaan.[5] Omdat ten tijde van het eerste informatieverzoek van de AP al aan een nieuwe website werd gewerkt, heeft zij de toen bestaande website aangeduid als 'oude website'.

De AP heeft de website – die inmiddels is vervangen door een andere – op 26 februari 2019 bezocht. Daarbij is geconstateerd dat de website, zoals vermeld, een formulier bevatte voor de inschrijving van nieuwe patiënten. Dit formulier bevatte velden voor onder meer de contactgegevens van de patiënt en diens ouders en het BSN van de patiënt. De AP heeft tevens geconstateerd dat de website ten tijde van het bezoek in het geheel geen gebruik maakte van een versleutelde verbinding. Dit blijkt uit de screenshots in bijlage 9 van het onderzoeksrapport, waarvan hieronder een uitsnede is opgenomen:

[3] https://www.ncsc.nl/onderwerpen/verbindingsbeveiliging.
[4] Bijvoorbeeld bij non-profit certificaatautoriteit Let's Encrypt, < https://letsencrypt.org/>. Er zijn certificaatautoriteiten die kostbare certificaten aanbieden (Extended Validation, of EV). Zulke certificaten bieden meer informatie over de partij aan wie het certificaat is verstrekt, maar leiden niet tot een andere of betere encryptie van uitgewisselde informatie.
[5] Brief van 19 augustus 2019, bijlage 8 bij het onderzoeksrapport.

Datum
4 februari 2021

Ons kenmerk
[vertrouwelijk]



Figuur 1: Uitsnede van de pagina-formatie van de website [url].

In het getoonde venster is onder het kopje “Technische details” een melding “Niet versleutelde verbinding” opgenomen. Deze melding luidt: “De website [url] ondersteunt geen versleuteling voor de pagina die u bekijkt. Gegevens die zonder versleuteling over het internet worden verzonden, kunnen onderweg door anderen worden ingezien.”

[Betrokkene] heeft erkend dat de oude website geen gebruik maakte van een versleutelde verbinding.[6] De ontwikkelaar van de oude website heeft haar nooit gewezen op die mogelijkheid. Anders had zij daar zeker gebruik van gemaakt, aldus [betrokkene].

Uit de brief van [betrokkene] van 19 augustus 2019 volgt dat als een formulier werd verzonden, de gegevens werden opgeslagen op de webserver waarop de oude website draaide. De orthodontiepraktijk kreeg daarvan een notificatie. Na het inloggen op de website werden de opgeslagen gegevens ingezien, overgenomen in de administratie van de praktijk en tot slot verwijderd van de webserver. Tussen juli 2018 en juni 2019 heeft de praktijk hooguit tien online inschrijvingen ontvangen, aldus [betrokkene].

[6] Zienswijze van 7 oktober 2019 op het voornemen tot oplegging van een bestuurlijke boete.

[Betrokkene] heeft de oude website op 29 mei 2019 offline laten halen.[7]

De AP heeft op 4 juli 2019 opnieuw de website van de orthodontiepraktijk bezocht en geconstateerd dat de website, inmiddels vernieuwd, wél gebruik maakte van een versleutelde verbinding, maar niet langer een online inschrijfformulier omvat. In plaats daarvan wordt nu een inschrijfformulier aangeboden in de vorm van een PDF-bestand, dat kan worden gedownload, uitgeprint, ingevuld, en afgeleverd bij de praktijk.

2.3.3. Beoordeling

De vraag of [betrokkene] de in artikel 32, eerste lid, van de AVG bedoelde passende technische en organisatorische maatregelen heeft getroffen moet – zoals vermeld onder 2.3.1 – worden beantwoord aan de hand van NEN 7510. Deze NEN-norm is voor het gebruik van het BSN verplicht gesteld en voor de zorg geldt dat deze norm ook overigens de geaccepteerde beveiligingsstandaarden bevat.

De AP stelt vast dat de oude website van de orthodontiepraktijk niet beschikte over een TLS-certificaat en daardoor geen gebruik maakte van het HTTPS-protocol. De communicatie met de website, waaronder het verzenden van een ingevuld inschrijvingsformulier, verliep daardoor over een niet-versleutelde en dus onbeveiligde verbinding. Hierdoor schepte het enkele beschikbaar hebben van het inschrijvingsformulier een verhoogd risico op een “man-in-the-middle-aanval”, waarbij verzonden informatie wordt onderschept en uitgelezen en/of gewijzigd, zonder dat de verzendende en ontvangende partij daar weet van hebben. Aldus staat vast dat [betrokkene] geen beheersmaatregelen heeft getroffen met betrekking tot communicatiebeveiliging. Dat is niet in overeenstemming met het bepaalde in NEN 7510 (waaronder de paragrafen 10.1 en 13.2).

Bedacht moet worden dat de patiënten van een orthodontiepraktijk in de regel minderjarige kinderen zijn. Dit volgt uit de aard van de behandeling, de velden van het inschrijfformulier (waarin wordt gevraagd om de gegevens van de ouders) en het beeldmateriaal op de website van de orthodontiepraktijk. Het zijn dus de gegevens van deze minderjarige kinderen die over de niet-versleutelde, onbeveiligde verbinding zijn verzonden. Daarbij komt dat het niet alleen gaat om het BSN, maar ook om gegevens die nauw verwant zijn aan de gezondheid van de desbetreffende patiënt.

Gelet op enerzijds de gevoelige aard van de gegevens die via het inschrijvingsformulier konden worden verzonden, en anderzijds de stand van de techniek en de daarmee samenhangende zeer geringe uitvoeringskosten van een versleutelde verbinding, is de conclusie dat [betrokkene] geen passende technische en organisatorische maatregelen heeft getroffen om de verwerking van persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking. Daarmee heeft zij artikel 32, eerste lid, van de AVG overtreden.

[7] Brief van 19 augustus 2019, bijlage 8 bij het onderzoeksrapport.

2.3.4. Zienswijze en reactie AP

[Betrokkene] heeft in haar zienswijze op het voornemen om een bestuurlijke boete op te leggen het volgende naar voren gebracht.

De ontwikkelaar van de oude website heeft [betrokkene] nooit gewezen op de mogelijkheid van een versleutelde verbinding. Als zij daarvan wist, had zij daarvan zeker gebruik gemaakt. Verder heeft zij actief geprobeerd om aan de AVG te voldoen, door om de twee jaar een audit te laten uitvoeren door een door de Nederlandse Vereniging van Orthodontisten aangewezen certificeringsbureau. Privacy maakt deel uit van de audit. Uit het laatste rapport, van juni 2017, blijkt dat de website is bekeken en dat daarover geen opmerkingen zijn gemaakt. Hetzelfde certificeringsbureau heeft in maart 2018 een stappenplan verstrekt om te voldoen aan de AVG. [Betrokkene] heeft dit plan punt voor punt afgewerkt, en hoewel aandacht is besteed aan privacy en informatiebeveiliging, is niet vermeld dat de website gebruik moet maken van een versleutelde verbinding. Verder wordt [betrokkene] om de vijf jaar gevisiteerd door collega-orthodontisten. Ook in het laatste visitatierapport is niet gewezen op het ontbreken van een versleutelde verbinding van de website. Er heeft niemand bij [betrokkene] geklaagd over de beveiliging en er is voor zover haar bekend geen schade geleden. Tot slot heeft [betrokkene] de oude website direct offline gehaald en opdracht gegeven de nieuwe website beter te beveiligen.

De zienswijze brengt de AP niet tot een ander standpunt over de geconstateerde overtreding. Een audit door een certificeringsbureau, een stappenplan in voorbereiding op het van toepassing worden van de AVG en een collegiale visitatie ontslaan [betrokkene], als verwerkingsverantwoordelijke, niet van de in artikel 32, eerste lid, van de AVG neergelegde verplichting om de in die bepaling bedoelde technische en organisatorische maatregelen te treffen. Dat anderen haar daar niet op hebben gewezen, terwijl zij ervan uitging dat dit waar nodig zou gebeuren, ontslaat haar niet van de eigen verantwoordelijkheid om actief zorg te dragen voor een technisch veilige verwerking van persoonsgegevens. Een organisatie die via internet persoonsgegevens van gevoelige aard en veelal van kinderen verwerkt, heeft een grote verantwoordelijkheid om zich ervan te vergewissen dat dergelijke persoonsgegevens ook veilig over het internet worden verzonden. Overigens blijkt uit de inhoud van het auditrapport en het verslag van de collegiale visitatie niet dat in het kader van de audit en visitatie aandacht is besteed aan de bescherming van persoonsgegevens. Dat er niemand bij [betrokkene] heeft geklaagd en dat haar geen schade bekend is, neemt verder evenmin weg dat zij onvoldoende technische en organisatorische beveiligingsmaatregelen heeft getroffen.

2.3.5. Conclusie

Gelet op het voorgaande is de AP van oordeel dat [betrokkene] artikel 32, eerste lid, van de AVG van 25 mei 2018 (het moment dat de AVG van toepassing werd) tot 29 mei 2019 heeft overtreden, omdat zij op de website van de orthodontiepraktijk een inschrijfformulier aanbood dat geen gebruik maakte van een versleutelde verbinding terwijl dat formulier was bedoeld om gevoelige persoonsgegevens uit te wisselen.

3. Bestuurlijke boete

3.1. Bevoegdheid van de AP tot het opleggen van een bestuurlijke boete

De AP is op grond van artikel 58, tweede lid, aanhef en onder i, gelezen in samenhang met artikel 83 van de AVG, bevoegd om een bestuurlijke boete op te leggen. Volgens artikel 83, eerste lid, dient een opgelegde boete doeltreffend, evenredig en afschrikwekkend te zijn. Uit het vierde lid van die bepaling volgt dat inbreuken op de verplichtingen van de verwerkingsverantwoordelijke (waaronder die vermeld in artikel 32 van de AVG) zijn onderworpen aan geldboeten tot € 10.000.000,00 of, voor een onderneming, tot 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is.

Op grond van artikel 14, derde lid, van de Uitvoeringswet Algemene verordening gegevensbescherming (hierna: UAVG) kan de AP in geval van overtreding van het bepaalde in artikel 83, vierde, vijfde of zesde lid, van de AVG een bestuurlijke boete opleggen van ten hoogste de in deze leden genoemde bedragen.

Bij de uitoefening van de bevoegdheid om een bestuurlijke boete op te leggen, hanteert de AP de Boetebeleidsregels Autoriteit Persoonsgegevens 2019 (hierna: Boetebeleidsregels 2019).[8]

3.2. Boetebeleidsregels Autoriteit Persoonsgegevens 2019

De relevante bepalingen van de Boetebeleidsregels 2019 zijn vermeld in de bijlage bij dit besluit. De systematiek van de Boetebeleidsregels 2019 is als volgt.

De overtredingen waarvoor de AP een boete kan opleggen tot het hierboven vermelde bedrag, zijn in de Boetebeleidsregels 2019 ingedeeld in drie boetecategorieën. Deze categorieën zijn gerangschikt naar zwaarte van de overtreding van de genoemde artikelen, waarbij categorie I de minst zware overtredingen bevat en categorie III de zwaarste overtredingen. Aan de categorieën zijn in hoogte oplopende geldboetes verbonden. Dit volgt uit artikel 2, onder 2.1 en 2.3 van de Boetebeleidsregels 2019.

Categorie I	Boetebandbreedte tussen € 0 en € 200.000	Basisboete: € 100.000
Categorie II	Boetebandbreedte tussen € 120.000 en € 500.000	Basisboete: € 310.000
Categorie III	Boetebandbreedte tussen € 300.000 en € 750.000	Basisboete: € 525.000

Volgens artikel 6 van de Boetebeleidsregels 2019 bepaalt de AP de hoogte van de boete door de basisboete naar boven of beneden bij te stellen, afhankelijk van de mate waarin de in artikel 7 genoemde factoren daartoe aanleiding geven. Op grond van artikel 8 is het mogelijk om de naast hogere of lagere categorie toe te passen als de voor de overtreding bepaalde boetecategorie in het concrete geval geen passende bestraffing toelaat.

[8] Gepubliceerd in Stcrt. 2019, 14586, 14 maart 2019.

3.3. Boetehoogte

De AP acht een boete van € 12.000,00 passend en geboden voor de hiervoor geconstateerde overtreding. In de navolgende paragrafen wordt dit als volgt onderbouwd. Allereerst ziet de AP aanleiding om de lagere boetecategorie I toe te passen. Er zijn geen boeteverlagende of -verhogende factoren van toepassing die nopen tot aanpassing van de voor die boetecategorie geldende basisboete van € 100.000,00. Ook de verwijtbaarheid van de gedraging geeft daartoe geen aanleiding. De AP ziet wel aanleiding om op grond van het evenredigheidsbeginsel de boete te matigen tot voormeld bedrag.

3.3.1. Boetecategorie en basisboete

De overtreding van artikel 32 van de AVG (beveiliging van de verwerking) is, blijkens bijlage I bij de Boetebeleidsregels 2019, ingedeeld in categorie II. Zoals volgt uit de tabel hiervoor, geldt voor deze categorie een boetebandbreedte van € 120.000,00 en € 500.000,00 en een basisboete van € 310.000,00. Deze boetebandbreedte en basisboete kunnen in dit geval niet leiden tot een passende bestraffing van de geconstateerde overtreding. Daarbij neemt de AP in aanmerking dat het onderzoek en de overtreding zien op het inschrijfformulier op de website van de praktijk, en niet op de patiëntenadministratie als zodanig. Het inschrijfformulier vormt technisch gezien een van die administratie losstaand systeem. De AP zal daarom op grond van artikel 8 van de Boetebeleidsregels 2019 categorie I toepassen (waarvoor een boetebandbreedte geldt van €0,00 tot € 200.000,00 en basisboete van € 100.000,00), en ook binnen die categorie de boetehoogte matigen op grond van hetgeen in deze en de navolgende paragrafen is overwogen.

De basisboete geldt als neutraal uitgangspunt, en dient te worden verhoogd of verlaagd voor zover de in artikel 7 van de Boetebeleidsregels 2019 vermelde factoren daartoe aanleiding geven. De uiteindelijke hoogte van de boete dient evenredig te zijn en afgestemd op de ernst van de overtreding en de mate waarin deze aan de overtreder kan worden verweten (vergelijk de artikelen 3:4 en 5:46 van de Algemene wet bestuursrecht; hierna: Awb). De in artikel 7 vermelde factoren geven op de volgende punten aanleiding tot opmerkingen. De niet besproken factoren zijn in dit geval niet van toepassing.

a. Aard, ernst en duur van de inbreuk

De website met het inschrijfformulier is volgens [betrokkene] op 27 oktober 2010 online gegaan en op 29 mei 2019 offline gehaald. Hoewel het formulier acht jaar en zeven maanden beschikbaar was voor gebruik, richtte het onderzoek van de AP zich op de periode van 25 mei 2018 tot 29 mei 2019. Daarmee sluit de AP aan bij de datum waarop de AVG van toepassing werd. Dat betekent dat de overtreding, voor zover deze in aanmerking wordt genomen, circa een jaar heeft geduurd.[9] De AP acht het ernstig dat de overtreding structureel en van lange duur was, te meer omdat [betrokkene] ook vóór het van toepassing

[9] Artikel 13 van de Wet bescherming persoonsgegevens (hierna: Wbp) is in materieel opzicht vergelijkbaar met artikel 32, eerste lid, van de AVG: beide bepalingen verplichten tot het treffen van technische en organisatorische maatregelen om een passend beveiligingsniveau te waarborgen. De invulling van artikel 13 van de Wbp is niet anders dan die van artikel 32 van de AVG, beschreven in de paragrafen 2.3.2 en 2.3.3. Ook in de periode dat de Wbp gold, was [betrokkene] dus in overtreding.

worden van de AVG, op grond van de Wet bescherming persoonsgegevens, verplicht was om een passend beveiligingsniveau te waarborgen. Die verplichting is dus niet eerst ontstaan bij het van toepassing worden van de AVG.

De AP rekent het [betrokkene] aan dat zij als professioneel zorgverlener in en in aanloop naar de onderzochte periode geen zorg heeft gedragen voor de in artikel 32, eerste lid, van de AVG bedoelde passende technische en organisatorische maatregelen, door middel van een correcte implementatie van NEN 7510. Voor het BSN geldt dat zij daartoe is verplicht op grond van de Regeling gebruik burgerservicenummer in de zorg. Voor de overige gegevens die via het formulier werden verzonden, geldt dat NEN 7510 de in de zorg algemeen geaccepteerde beveiligingsstandaarden bevat. [Betrokkene] had hier uit hoofde van haar hoedanigheid als zorgverlener van op de hoogte moeten zijn.

[Betrokkene] heeft verder niet slechts de theoretische mogelijkheid gecreëerd dat het formulier zou worden gebruikt om gevoelige gegevens over een onbeveiligde verbinding te verzenden. Gebleken is immers dat het formulier ook daadwerkelijk is gebruikt. Voor elke inzending geldt dat daarmee het belang dat de geschonden norm beoogt te beschermen, in het geding is gekomen. Hoewel het exacte aantal inzendingen van het formulier niet meer valt vast te stellen, acht de AP het niet onwaarschijnlijk dat het formulier ook is gebruikt toen de Wbp van toepassing was, waaronder ook al een passend beveiligingsniveau was vereist.

De AP rekent het [betrokkene] aan dat de overtreding lang heeft geduurd en in strijd was met de normen die specifiek gelden voor haar beroepsgroep (de zorg). Dat de overtreding ook daadwerkelijk heeft geleid tot het herhaaldelijk verzenden van gevoelige gegevens over een onbeveiligde verbinding acht de AP extra kwalijk.

g. De categorieën persoonsgegevens waarop de inbreuk betrekking heeft

Via het inschrijfformulier werd allereerst gevraagd om het BSN. Dat is op zichzelf al een gevoelig gegeven, maar dat geldt te meer als het gegeven wordt bezien in samenhang met de overige gevraagde gegevens. De gevoeligheid blijkt ook uit de wettelijke verplichting om bij de verwerking van het BSN te voldoen aan NEN 7510. De gegevens in samenhang bezien bieden zoveel informatie over de in te schrijven patiënt, dat het risico op identiteitsfraude bestaat als de gegevens zouden worden onderschept. De AP neemt daarbij ook in aanmerking dat het veelal ging om de gegevens van minderjarigen, zoals vermeld in paragraaf 2.3.3.

Verder zijn de andere gevraagde gegevens evenzeer van gevoelige aard, omdat zij nauw verband houden met de gezondheid van de in te schrijven patiënt. Dat geldt overigens ook voor de inschrijving bij een orthodontist als zodanig. De AP heeft, mede omdat de verwerking niet meer plaatsvindt, niet onderzocht of dit kwalificeert als bijzondere persoonsgegevens als bedoeld in artikel 9 van de AVG, maar volstaat met de constatering dat het formulier is gebruikt om gevoelige persoonsgegevens te verzenden.

De AP rekent het [betrokkene] aan dat de overtreding betrekking heeft op gevoelige gegevens van minderjarigen.

Verhoging of verlaging basisboete

Gelet op het voorgaande ziet de AP in de factoren vermeld in de Boetebeleidsregels 2019, voor zover van toepassing in het voorliggende geval, geen aanleiding om de basisboete te verlagen. Van aanleiding om het boetebedrag te verhogen is evenmin sprake.

3.3.2. Verwijtbaarheid van de gedraging

Op grond van artikel 5:46, tweede lid, van de Awb houdt de AP bij het opleggen van een bestuurlijke boete rekening met de mate waarin deze aan de overtreder kan worden verweten. Omdat het in dit geval gaat om een overtreding, is voor het opleggen van een bestuurlijke boete conform vaste rechtspraak niet vereist dat wordt aangetoond dat sprake is van opzet en mag de AP verwijtbaarheid veronderstellen als het daderschap vaststaat.[10]

[Betrokkene] heeft, zoals vermeld in paragraaf 2.3.4, in haar zienswijze gewezen op een auditrapport, stappenplan ter voorbereiding op de AVG en een rapport van een collegiale visitatie. Volgens [betrokkene] is zij in geen van deze stukken gewezen op de tekortkoming met betrekking tot het online inschrijfformulier. Voor zover [betrokkene] bedoelt dat hierom sprake is van verminderde verwijtbaarheid, volgt de AP haar niet. Zij had als zorgverlener beroepshalve bekend moeten zijn met de voor die zorg geldende beveiligingsnormen. Dat anderen haar niet op de tekortkoming hebben gewezen, doet niet af aan haar eigen verplichtingen als verwerkingsverantwoordelijke.

Nu de overtreding [betrokkene] ten volle kan worden verweten, geeft de verwijtbaarheid van de overtreding geen aanleiding om het boetebedrag te verlagen.

3.3.3. Evenredigheid

Tot slot zal de AP op grond van de artikelen 3:4 en 5:46 van de Awb (evenredigheidsbeginsel) beoordelen of de toepassing van haar beleid voor het bepalen van de hoogte van de boete, gezien de omstandigheden van het concrete geval, niet tot een onevenredige uitkomst leidt.

De AP acht het in het licht van de evenredigheid van de op te leggen boete van belang dat de overtreding, zoals vermeld in paragraaf 3.3.1, ziet op het niet beveiligde gebruik van een inschrijfformulier op de website van de praktijk, en niet op de gehele patiëntenadministratie. De AP heeft over het gebruik van de onbeveiligde verbinding één klacht ontvangen. De AP heeft over de patiëntenadministratie zelf geen signalen ontvangen en heeft daar dan ook geen onderzoek naar gedaan. Verder is het gebruik van het inschrijfformulier in de in aanmerking genomen periode beperkt gebleven.

[10] Vergelijk de uitspraken van het CBb van 29 oktober 2014 (ECLI:NL:CBB:2014:395, ow. 3.5.4), 2 september 2015 (ECLI:NL:CBB:2015:312, ow. 3.7) en 7 maart 2016 (ECLI:NL:CBB:2016:54, ow. 8.3). Vergelijk ook de uitspraken van de Afdeling bestuursrechtspraak van 29 augustus 2018 (ECLI:NL:RVS:2018:2879, ow. 3.2) en 5 december 2018 (ECLI:NL:RVS:2018:3969, ow. 5.1). Zie tot slot *Kamerstukken II* 2003/04, 29 702, nr. 3, p. 134.

Daarnaast is van belang dat de onderneming van [betrokkene] moet worden gerekend tot het midden- en kleinbedrijf (MKB). Ook is het, gelet op de geringe kosten die gepaard gaan met het beveiligd verzenden van een formulier (vergelijk paragraaf 2.3.1), niet aannemelijk dat als gevolg van de overtreding financiële winsten zijn gemaakt of verliezen zijn vermeden.

De AP ziet in het geheel van de vermelde omstandigheden aanleiding om het basisbedrag van € 100.000,00 te matigen. De AP acht, mede gelet op de ernst van de overtreding, de substantiële draagkracht van de onderneming en de doelgroep waarvan de persoonsgegevens worden verwerkt, een boete van € 12.000,00 passend en geboden.

De AP dient tot slot te bezien of in hetgeen [betrokkene] naar voren heeft gebracht in haar zienswijze op het voornemen om handhavend op te treden, aanleiding ligt om aan te nemen dat deze boete tot een onevenredige uitkomst zou leiden.

[Betrokkene] heeft in haar zienswijze gesteld dat zij een boete ter hoogte van het basisbedrag van boetecategorie II (€ 310.000,00) nooit zou kunnen betalen. Ter staving van die stelling heeft zij een voorlopige aanslag inkomstenbelasting over 2018 overgelegd. In paragraaf 3.3.1 is evenwel uiteengezet dat niet boetecategorie II wordt toegepast, maar boetecategorie I. Het daarbij behorende basisbedrag is bovendien hiervoor gematigd tot € 12.000,00. Uit de door [betrokkene] overgelegde stukken volgt niet dat deze boete onevenredige gevolgen zou hebben, bijvoorbeeld doordat de orthodontiepraktijk in het voortbestaan zou worden bedreigd. De AP ziet in de draagkracht van [betrokkene] dan ook geen aanleiding om de boete verder te matigen.

3.4. Conclusie

De AP stelt het boetebedrag voor de overtreding van artikel 32, eerste lid, van de AVG, gelet op het voorgaande vast op € 12.000,00.

Datum
4 februari 2021

Ons kenmerk
[vertrouwelijk]

4. Dictum

Boete
De AP legt aan [betrokkene], handelend onder de naam [onderneming], wegens overtreding van artikel 32, eerste lid, van de AVG een bestuurlijke boete op ten bedrage van € 12.000,00 (zegge: twaalfduizend euro).[11]

Hoogachtend,
Autoriteit Persoonsgegevens,

drs. C.E. Mur
Bestuurslid

Rechtsmiddelenclausule
Indien u het niet eens bent met dit besluit, kunt u binnen zes weken na de datum van verzending van het besluit digitaal of op papier een bezwaarschrift indienen bij de Autoriteit Persoonsgegevens. Ingevolge artikel 38 van de Uitvoeringswet AVG schort het indienen van een bezwaarschrift de werking van de beschikking tot oplegging van de bestuurlijke boete op. Vermeld in uw bezwaarschrift ten minste:

- uw naam en adres;
- de datum van uw bezwaarschrift;
- het in deze brief genoemde kenmerk (zaaknummer), of voeg een kopie van dit besluit bij;
- de reden(en) waarom u het niet eens bent met dit besluit;
- uw handtekening.

U kunt het bezwaarschrift digitaal indienen via de website. Ga naar www.autoreitpersoonsgegevens.nl, en klik onderaan de pagina, onder het kopje “Contact met de Autoriteit Persoonsgegevens”, op de link “Bezwaar maken tegen een besluit”. Vanaf daar gebruikt u het “Formulier bezwaarschrift”.

Stuurt u het bezwaarschrift liever per post op? Dan kan dat naar het volgende adres:

Autoriteit Persoonsgegevens
Directie Juridische zaken & Wetgevingsadvies, afdeling Bezwaar
Postbus 93374
2509 AJ DEN HAAG

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

Datum
4 februari 2021

Ons kenmerk
[vertrouwelijk]

BIJLAGE – Wettelijk kader

Algemene verordening gegevensbescherming (AVG)

Artikel 2 (Materieel toepassingsgebied

1. Deze verordening is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

[…]

Artikel 3 (Territoriaal toepassingsgebied

1. Deze verordening is van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Unie, ongeacht of de verwerking in de Unie al dan niet plaatsvindt.

[…]

Artikel 4 (Definities)

Voor de toepassing van deze verordening wordt verstaan onder:

1) "persoonsgegevens": alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;
2) "verwerking": een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;

[…]

7) "verwerkingsverantwoordelijke": een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;

[…]

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.

[…]

Artikel 58 (Bevoegdheden)

[…]

2. Elk toezichthoudende autoriteit heeft alle volgende bevoegdheden tot het nemen van corrigerende maatregelen:
   […]
   i) naargelang de omstandigheden van elke zaak, naast of in plaats van de in dit lid bedoelde maatregelen, een administratieve geldboete opleggen op grond van artikel 83; en
   […]

[…]

Artikel 83 (Algemene voorwaarden voor het opleggen van administratieve geldboeten)

1. Elke toezichthoudende autoriteit zorgt er voor 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, naar gelang 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 verwerkings-verantwoordelijke 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.

[…]

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;
   […]

[…]

Uitvoeringswet Algemene verordening gegevensbescherming

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.

[…]

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.

[…]

Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg[12]

Artikel 8
1. De zorgaanbieder neemt het burgerservicenummer van de cliënt in zijn administratie op bij het vastleggen van persoonsgegevens met betrekking tot de verlening van zorg.

[…]

Artikel 10
Bij ministeriële regeling kan worden bepaald aan welke beveiligingseisen de gegevensverwerking, bedoeld in de artikelen 8 en 9, voldoet.

Regeling gebruik burgerservicenummer

Artikel 1
In deze regeling wordt verstaan onder:
a. Minister: Minister van Volksgezondheid, Welzijn en Sport;
b. wet: Wet gebruik burgerservicenummer in de zorg;[13]
c. besluit: Besluit gebruik burgerservicenummer in de zorg;
d. NEN: door de Stichting Nederlands Normalisatie-Instituut uitgegeven norm;
e. NEN 7510: NEN 7510 en de uitwerkingen daarvan in de NEN 7511 en de NEN 7512;

[…]

Artikel 2
De gegevensverwerking, bedoeld in de artikelen 8 en 9 van de wet […] voldoet aan de NEN 7510.

**NEN 7510-2: Medische informatica – Informatiebeveiliging in de zorg –
Deel 2: Beheersmaatregelen**

10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen

Beheersmaatregel
Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.

[…]

Bij het implementeren van het cryptografiebeleid behoort rekening te worden gehouden met de regelgeving en nationale beperkingen die kunnen gelden voor het gebruik van cryptografische technieken in verschillende delen van de wereld en met problemen met grensoverschrijdende

[12] Tot 1 juli 2017 heette deze wet de Wet gebruik burgerservicenummer in de zorg.
[13] Zoals vermeld in de bovenstaande voetnoot, heet deze wet thans de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg.

stromen van versleutelde informatie (zie 18.1.5).

Cryptografische beheersmaatregelen kunnen worden gebruikt voor verschillende informatiebeveiligingsdoelstellingen, bijv.:

a) vertrouwelijkheid: codering van informatie gebruiken om gevoelige of essentiële informatie, tijdens opslag of verzending, te beschermen;
[…]

Overige informatie
Besluitvorming over het punt of een cryptografische oplossing passend is, behoort te worden beschouwd als deel van het totale proces van risicobeoordeling en het kiezen van beheersmaatregelen.
[…]

Voor het kiezen van de juiste cryptografische beheersmaatregelen die voldoen aan de doelstellingen van het informatiebeveiligingsbeleid behoort deskundig advies te worden ingewonnen.

13.2.1 Beleid en procedures voor informatietransport

Beheersmaatregel
Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.
Implementatierichtlijn
Bij procedures die moeten worden gevolgd en beheersmaatregelen die moeten worden uitgevoerd bij het gebruik van communicatiefaciliteiten voor informatietransport behoren de volgende punten in overweging te worden genomen:

a) procedures die zijn ontworpen ter beveiliging van overgedragen informatie tegen interceptie, kopiëren, wijziging, foutieve routering en vernietiging;
[…]
f) gebruik van cryptografische technieken, bijv. om de vertrouwelijkheid, integriteit en authenticiteit van informatie te beschermen (zie hoofdstuk 10);
[…]

ZORGSPECIFIEKE IMPLEMENTATIERICHTLIJN
Organisaties behoren te garanderen dat de beveiliging van dergelijke uitwisseling van informatie het onderwerp is van beleidsontwikkeling en van audits van de naleving ervan (zie hoofdstuk 18).
[…]

Datum
4 februari 2021

Ons kenmerk
[vertrouwelijk]

Boetebeleidsregels Autoriteit Persoonsgegevens 2019

Artikel 2. Categorie-indeling en boetebandbreedtes

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

[…]

2.3 De Autoriteit Persoonsgegevens stelt de basisboete voor overtredingen waarvoor een wettelijk boetemaximum geldt van € 10.000.000 of, voor een onderneming, tot 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is, dan wel € 20.000.000 of, voor een onderneming, tot 4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is, vast binnen de volgende boetebandbreedtes:

Categorie I	Boetebandbreedte tussen € 0 en € 200.000	Basisboete: € 100.000
Categorie II	Boetebandbreedte tussen € 120.000 en € 500.000	Basisboete: € 310.000
Categorie III	Boetebandbreedte tussen € 300.000 en € 750.000	Basisboete: € 525.000

[…]

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

Artikel 6. De basisboete en mogelijke verhoging of verlaging

De Autoriteit Persoonsgegevens bepaalt de hoogte van de boete door het bedrag van de basisboete naar boven (tot ten hoogste het maximum van de bandbreedte van de aan een overtreding gekoppelde boetecategorie) of naar beneden (tot ten laagste het minimum van die bandbreedte) bij te stellen. De basisboete wordt verhoogd of verlaagd afhankelijk van de mate waarin de factoren die zijn genoemd in artikel 7 daartoe aanleiding geven.

Artikel 7. Relevante factoren

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

a) 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 van de Algemene verordening gegevensbescherming;
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, tweede lid, van de Algemene verordening gegevensbescherming 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 van de Algemene verordening gegevensbescherming of van goedgekeurde certificeringsmechanismen overeenkomstig artikel 42 van de Algemene verordening gegevensbescherming; 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.

Artikel 8. Buiten de bandbreedte treden en verhoogde boetemaxima voor een onderneming

8.1 Indien de voor de overtreding bepaalde boetecategorie in het concrete geval geen passende bestraffing toelaat, kan de Autoriteit Persoonsgegevens bij het bepalen van de hoogte van de boete de boetebandbreedte van de naast hogere categorie respectievelijk de boetebandbreedte van de naast lagere categorie toepassen

Bijlage 1, behorende bij artikel 2

Overtredingen met een wettelijk boetemaximum van € 10.000.000 of, voor een onderneming, tot 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is:

Wetsartikel	Omschrijving	Categorie
Algemene verordening gegevensbescherming		
[…]	[…]	[…]
artikel 32	beveiliging van de verwerking	II
[…]	[…]	[…]