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
Coöperatie VGZ U.A.
De Voorzitter van de Raad van Bestuur
De heer drs. R. Kliphuis
Postbus 5040
6802 EA ARNHEM

Datum
15 februari 2018

Ons Kenmerk
[VERTROUWELIJK]

Contactpersoon
[VERTROUWELIJK]
070 8888 500

Onderwerp
Last onder dwangsom en definitieve bevindingen

Geachte heer Kliphuis,

Hieronder treft u het besluit aan van de Autoriteit Persoonsgegevens (AP) tot oplegging van een last onder dwangsom aan Coöperatie VGZ U.A. (VGZ). Dit besluit maakt onderdeel uit van het nieuwe besluit van heden op het bezwaar van Burgerrechtenvereniging Vrijbit (Vrijbit). Dit nieuwe besluit op bezwaar is genomen na het onderzoek dat de AP heeft uitgevoerd naar aanleiding van de tussenuitspraak van de rechtbank Midden Nederland (de rechtbank) van 7 juli 2017, ECLI:NL:RBMNE:2017:3421 (de tussenuitspraak). Deze zaak is aangevangen met een handhavingsverzoek dat Vrijbit bij het College bescherming persoonsgegevens (CBP) heeft ingediend.

Het handhavingsverzoek van Vrijbit heeft betrekking op de wijze waarop Nederlandse zorgverzekeraars op dit moment persoonsgegevens betreffende de gezondheid verwerken. Volgens Vrijbit is deze werkwijze in strijd met de Wet bescherming persoonsgegevens (Wbp), het Handvest van de grondrechten van de Europese Unie (het Handvest) en artikel 8 van het Verdrag voor de rechten van de mens en de fundamentele vrijheden (EVRM). Vrijbit legt hieraan samengevat ten grondslag dat zorgverzekeraars nog altijd werken volgens de Gedragscode Verwerking Persoonsgegevens Zorgverzekeraars (de gedragscode), terwijl de AP aan die gedragscode alsnog haar goedkeuring heeft onthouden naar aanleiding van een uitspraak van de rechtbank Amsterdam uit 2013.[1]

Het verloop van de procedure tussen Vrijbit en de AP, het wettelijk kader, de uitspraak van de rechtbank Amsterdam, de tussenuitspraak, het oorspronkelijke besluit op bezwaar van 1 juni 2016, de opzet van het onderzoek en het verloop van het onderzoek zijn uiteengezet in het nieuwe besluit op bezwaar. De AP verwijst hier kortheidshalve naar.

[1] Rechtbank Amsterdam 13 november 2013, ECLI:NL:RBAMS:2013:7480.

Bevindingen

1 Als **bijlage** bij dit besluit tot oplegging van de last onder dwangsom zijn de bevindingen van de AP gevoegd. Hierin komt allereerst de gedragscode en het door VGZ gehanteerde privacybeleid aan de orde (1). Daarna wordt ingegaan op de aspecten digitale declaratie zonder diagnose-informatie (2), doelbinding (3), ongeautoriseerde toegang tot persoonsgegevens (4), bewerkers (5) en medisch beroepsgeheim (6).

2 In de bevindingen komt de AP tot de conclusie dat VGZ artikel 13 van de Wbp overtreedt. De AP heeft in dat kader het volgende geconstateerd:

- VGZ heeft haar bedrijfscultuur organisatorisch zo ingericht dat uitsluitend medewerkers toegang mogen hebben tot persoonsgegevens betreffende de gezondheid voor zover dat noodzakelijk is voor het doeleinde waarvoor de medewerkers de persoonsgegevens verwerken. Zo is onder meer door VGZ vastgelegd dat marketingmedewerkers geen persoonsgegevens betreffende de gezondheid mogen verwerken.
- Uit het onderzoek van de AP blijkt echter dat een aantal medewerkers van de afdeling Klant en Merkpartners van VGZ feitelijk toegang hebben tot persoonsgegevens betreffende de gezondheid, terwijl dit voor hun werkzaamheden niet noodzakelijk is. Het kunnen raadplegen van persoonsgegevens is ingevolge artikel 1, aanhef en onder b, van de Wbp aan te merken als het verwerken van persoonsgegevens.
- VGZ beschikt dan ook niet over afdoende technische middelen waarmee geborgd is dat medewerkers geen toegang hebben gehad tot persoonsgegevens die niet noodzakelijk zijn voor het doeleinde waarvoor zij worden verwerkt. In dit kader wijst de AP er verder op dat VGZ geen logbestanden bijhoudt over de toegang tot bijzondere persoonsgegevens.
- Het voorgaande leidt tot de conclusie dat VGZ niet beschikt over passende technologische maatregelen als bedoeld in artikel 13 van de Wbp;
- De AP heeft in de overgelegde stukken die weergeven op welke wijze een marketingactie bij VGZ wordt uitgevoerd overigens geen aanwijzingen aangetroffen voor de conclusie dat marketingmedewerkers daadwerkelijk persoonsgegevens betreffende de gezondheid verwerken voor een marketingactie. Dat doet evenwel niet af aan de conclusie dat artikel 13 van de Wbp is overtreden, omdat de *technologische* maatregelen die VGZ heeft getroffen, niet passend zijn.

Beginselplicht tot handhaving

3 Uit artikel 65 van de Wbp, in samenhang bezien met artikel 5:32, eerste lid, van de Algemene wet bestuursrecht (Awb) volgt dat de AP bevoegd is om een last onder dwangsom op te leggen bij overtreding van artikel 13 van de Wbp.
Ingevolge artikel 5:2, eerste lid, aanhef en onder b, van de Awb is de last onder dwangsom gericht op het beëindigen van de geconstateerde overtreding en het voorkomen van herhaling.

4 Gelet op het algemeen belang dat is gediend met handhaving, zal de AP in geval van een overtreding van een wettelijk voorschrift in de regel van haar handhavende bevoegdheid gebruik moeten maken. Bijzondere omstandigheden in verband waarmee van handhavend optreden moet worden afgezien, doen zich in dit geval niet voor.

Last onder dwangsom en begunstigingstermijn

5 De AP gelast VGZ haar systeem op zodanige wijze in te richten dat ongeautoriseerde toegang tot persoonsgegevens wordt voorkomen.

Zij dient daartoe in ieder geval:

1. De autorisaties en raadpleegrollen die VGZ hanteert voor de logische toegangsbeveiliging van systemen van de afdeling Klant en Merkpartners dienen te worden aangepast, meer bepaaldelijk voor de in vertrouwelijke bijlage 1 vermelde medewerkers. Deze autorisaties en raadpleegrollen van de genoemde medewerkers van VGZ dienen zodanig te worden aangepast, dat deze medewerkers feitelijk geen toegang meer hebben tot persoonsgegevens, waaronder persoonsgegevens betreffende de gezondheid, wanneer de verwerking van deze persoonsgegevens niet noodzakelijk is voor hun werkzaamheden.
2. Zorg te dragen voor adequate technologische controlesystemen op basis waarvan zij borgt dat medewerkers uitsluitend toegang hebben tot bijzondere persoonsgegevens, waaronder persoonsgegevens betreffende de gezondheid, wanneer die toegang noodzakelijk is voor de werkzaamheden van een medewerker. Het gaat hierbij in ieder geval om logging van toegang en mutaties, zodat – al dan niet naar aanleiding van incidenten – gecontroleerd kan worden of medewerkers toegang hebben verkregen terwijl de toegang tot deze gegevens niet noodzakelijk is voor hun werkzaamheden.
3. VGZ dient voorts te zorgen voor een periodieke schriftelijke terugkoppeling – die ten minste eenmaal per half jaar plaatsvindt – door de Functionaris voor de Gegevensbescherming en de Compliance officer(s) aan de directie waaruit blijkt of zich incidenten hebben voorgedaan en zo ja, welke maatregelen zijn getroffen:
   a. ten aanzien van het vermelde onder 1;
   b. ten aanzien van het vermelde onder 2.

-begunstigingstermijn en hoogte dwangsom t.a.v. onderdelen 2 en 3b

6 Gelet op hetgeen VGZ naar voren heeft gebracht over haar wens om haar systeem zo in te richten dat technisch en grotendeels geautomatiseerd wordt geborgd dat medewerkers geen toegang hebben tot meer persoonsgegevens dan noodzakelijk is voor hun werkzaamheden, verbindt de AP aan onderdeel 2 en onderdeel 3b van deze last een begunstigingstermijn die eindigt op **31 december 2018.**

7 Indien VGZ niet vóór het einde van de onder 6 vermelde begunstigingstermijn aan de last voldoet, verbeurt zij een dwangsom. De AP stelt de hoogte van deze dwangsom vast op een bedrag van € 150.000,00 voor iedere (gehele) week, na afloop van de laatste dag van de gestelde termijn, waarop VGZ nalaat aan onderdeel 2 en onderdeel 3b van de last te voldoen, tot een maximum van **€ 750.000,00.** Gelet op het feit dat de dwangsom een prikkel dient te zijn tot naleving van de last, de hoogte van de omzet van VGZ, het grote aantal verzekerden en de ernst van de overtreding, acht de AP de hoogte van deze dwangsom passend.

-begunstigingstermijn en hoogte dwangsom t.a.v. onderdelen 1 en 3a

8 Wat betreft onderdeel 1. van deze last is de AP van oordeel dat met de uitvoering daarvan minder inspanningen gemoeid zijn. De AP verbindt daarom aan onderdeel 1 en onderdeel 3a van de last een begunstigingstermijn die eindigt op **26 mei 2018.**

9 Indien VGZ niet vóór het einde van de onder 8 vermelde begunstigingstermijn aan de last voldoet, verbeurt zij een dwangsom. De AP stelt de hoogte van deze dwangsom vast op een bedrag van € 50.000,00 voor iedere (gehele) week, na afloop van de laatste dag van de gestelde termijn, waarop VGZ nalaat aan onderdeel 1 en onderdeel 3a van de last te voldoen, tot een maximum van **€ 250.000,00.**
Gelet op het feit dat de dwangsom een prikkel dient te zijn tot naleving van de last, de hoogte van de omzet van VGZ, het grote aantal verzekerden en de ernst van de overtreding, acht de AP de hoogte van deze dwangsom passend.

-tussentijdse rapportage

10 De AP raadt VGZ aan om aan de hand van een concrete planning – eenmaal per kwartaal – mededeling te doen aan de AP over de voortgang van de maatregelen die zij neemt om te kunnen voldoen aan de opgelegde last.

-nacontrole

11 De AP verzoekt VGZ tijdig vóór het einde van de begunstigingstermijn bewijsstukken aan de AP toe te zenden waaruit blijkt dat tijdig en volledig aan de last wordt voldaan. Het tijdig overleggen van bewijsstukken laat overigens onverlet dat de AP bevoegd is om een onderzoek, waaronder een onderzoek ter plaatse, in te stellen indien het dit dienstig voorkomt.

Toelichting op de last

12 Ter toelichting merkt de AP het volgende op.

13 In het document 'CBP Richtsnoeren. Beveiliging van persoonsgegevens' (*Stcrt.* 2013, 5174, hierna ook: de richtsnoeren) is invulling gegeven aan de vraag wanneer beveiligingsmaatregelen 'passend' in de zin van artikel 13 van de Wbp zijn. In de richtsnoeren wordt duidelijk gemaakt dat voor die beoordeling allereerst moet worden gekeken naar de te stellen betrouwbaarheidseisen. Hierbij moet aan de hand van de aard van de te beschermen gegevens worden vastgesteld wat een passend beschermingsniveau is. De aard van de persoonsgegevens is hierbij van belang. Ook de hoeveelheid verwerkte persoonsgegevens per persoon en het doel waarvoor de persoonsgegevens worden verwerkt, moet hierbij worden meegewogen.

14 In dit geval gaat het om de verwerking van gegevens betreffende de gezondheid, zijnde bijzondere persoonsgegevens. Dat betekent dat de gevolgen van een onrechtmatige verwerking van die gegevens, voor betrokkenen ernstig kunnen zijn. Als gevolg hiervan is voor de verwerking van persoonsgegevens door VGZ een hoog beveiligingsniveau vereist.

15 Na het vaststellen van de betrouwbaarheidseisen moet de verantwoordelijke passende beveiligingsmaatregelen treffen, die waarborgen dat aan de betrouwbaarheidseisen wordt voldaan, zo staat in de richtsnoeren. Beveiligingsstandaarden geven houvast bij het daadwerkelijk treffen van

passende maatregelen om de risico's af te dekken. Een zeer veel gebruikte beveiligingsstandaard is de Code voor Informatiebeveiliging, NEN-ISO/IEC 27002+C1(2014)+C2 (2015). Hierin zijn concrete beveiligingsmaatregelen opgenomen. Beveiligingsstandaarden geven houvast bij het daadwerkelijk treffen van passende maatregelen om de risico's af te dekken. Welke beveiligingsstandaarden voor een bepaalde verwerking relevant zijn en welke beveiligingsmaatregelen op grond van deze beveiligingsstandaarden moeten worden getroffen, moet echter van geval tot geval worden bepaald.

16 In de Code voor Informatiebeveiliging zijn de volgende in dit verband relevante maatregelen genoemd:
9.4.1 Beperking toegang tot informatie
Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.
12.4.1 Gebeurtenissen registreren
Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.

17 Los van de inrichting van het beleid voor toegangsbeveiliging rechtvaardigt de aard van de persoonsgegevens die een zorgverzekeraar als VGZ verwerkt en de omvang van die verwerking, dat ten minste op zodanige wijze logbestanden worden bijgehouden dat in ieder geval een reactieve controle van de logbestanden mogelijk is. In het bijzonder gaat het de AP erom dat handelingen in de vorm van raadplegingen of mutaties in de systemen waartoe medewerkers geautoriseerd zijn met betrekking tot (bijzondere) persoonsgegevens niet worden gelogd, als gevolg waarvan een controle op de toegang tot die gegevens – bijvoorbeeld naar aanleiding van incidenten – thans niet mogelijk is.

18 De AP heeft, zoals hiervoor is opgemerkt, tijdens het onderzoek geconstateerd dat een aantal medewerkers van de afdeling Klant en Merkpartners autorisaties hebben die toegang geven tot persoonsgegevens betreffende de gezondheid, terwijl dit voor hun werkzaamheden niet noodzakelijk is. VGZ heeft in haar reactie op het voornemen tot handhaving de juistheid van deze bevinding erkend. VGZ heeft verklaard dat zij correctieve maatregelen heeft genomen, als gevolg waarvan de onterechte toegang is beëindigd. Reeds omdat deze verklaring niet is geadstrueerd met bewijs, ziet de AP geen aanleiding om op dit punt af te zien van handhaving.

19 VGZ heeft voorts naar voren gebracht dat de AP in haar voorlopige bevindingen ten onrechte een koppeling heeft gemaakt tussen logging en het voorkomen van ongeautoriseerde toegang tot persoonsgegevens. In reactie hierop wijst de AP op het volgende. De AP heeft hiervoor onder 17 reeds uiteengezet dat en waarom het bijhouden van logbestanden voor een zorgverzekeraar als VGZ een noodzakelijke maatregel is om een passend beveiligingsniveau te garanderen. Dit geldt voor VGZ temeer, nu zij een beleid voor toegangsbeveiliging heeft dat inhoudt dat wordt gewerkt met een autorisatiematrix per functionaris. Dit brengt het risico mee dat de feitelijk toegekende autorisaties na verloop van tijd niet langer overeenkomen met de autorisaties die strikt noodzakelijk zijn voor de werkzaamheden van de desbetreffende medewerker.
Hoewel de AP niet heeft vastgesteld dat andere medewerkers van VGZ beschikken over autorisaties en rollen die een verdergaande toegang tot (bijzondere) persoonsgegevens mogelijk maken dan noodzakelijk is, heeft de AP VGZ evenwel de **aanbeveling** gedaan om het autorisatiebeleid zo uit te werken dat als

hoofdregel geldt dat per functie(groep) wordt vastgelegd welke rollen en autorisaties voor de uitoefening van die functie noodzakelijk zijn.

20 Wat betreft de begunstigingstermijn, heeft VGZ voorgesteld om uiterlijk 1 maart 2019 de benodigde maatregelen te treffen om aan de last te kunnen voldoen. VGZ heeft gesteld dat zij hierbij afhankelijk is van derde partijen. VGZ heeft dit niet aan de hand van een onderbouwde planning inzichtelijk gemaakt. Gezien de ernst van de overtreding en naar inschatting van de AP te treffen maatregelen, acht de AP de hiervoor onder 6 en 8 vermelde termijnen passend en redelijk.

21 Hetgeen VGZ in haar reactie op het voornemen tot handhaving op dit punt naar voren heeft gebracht, vormt gelet op het voorgaande voor de AP geen reden om af te zien van handhavend optreden.

Datum
15 februari 2018

Ons Kenmerk
[VERTROUWELIJK]

Ter voorlichting van partijen

22 Het besluit op bezwaar van heden met kenmerk z2016-12335 en het onderhavige besluit tot oplegging van de last onder dwangsom en vormen tezamen het besluit van de AP op het bezwaar van Vrijbit. Tegen dit besluit staat beroep open bij de rechtbank.

Een afschrift van deze brief zal worden verzonden aan de Functionaris voor de Gegevensbescherming van VGZ, [VERTROUWELIJK].

Hoogachtend,
Autoriteit Persoonsgegevens,

w.g.

mr. A. Wolfsen
Voorzitter

Rechtsmiddel

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 Midden-Nederland, waar reeds deze procedure aanhangig is. U dient een afschrift van dit besluit mee te zenden. Het indienen van een beroepschrift schort de werking van dit besluit niet op.