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 Menzis U.A.
Voorzitter Raad van Bestuur
De heer drs. R. Wenselaar
Postbus 75000
7500 KC Enschede

Datum	Ons kenmerk	Uw kenmerk
15 februari 2018	[VERTROUWELIJK]	20171025/RvB/jd

Contactpersoon
[VERTROUWELIJK]
070 8888 500

Onderwerp
Last onder dwangsom en definitieve bevindingen

Geachte heer Wenselaar,

Hieronder treft u het besluit aan van de Autoriteit Persoonsgegevens (AP) tot oplegging van een last onder dwangsom aan Coöperatie Menzis U.A. (Menzis). 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.

Datum
15 februari 2018

Ons kenmerk
[VERTROUWELIJK]

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 Menzis 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).

Overtreding

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

- Menzis 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 Menzis vastgelegd dat marketingmedewerkers geen persoonsgegevens betreffende de gezondheid mogen verwerken.
- Uit het onderzoek van de AP blijkt echter dat marketingmedewerkers van Menzis feitelijk wel toegang hebben tot persoonsgegevens betreffende de gezondheid. Het kunnen raadplegen van persoonsgegevens is ingevolge artikel 1, aanhef en onder b, van de Wbp aan te merken als het verwerken van persoonsgegevens.
- Menzis beschikt dan ook niet over afdoende technische middelen waarmee wordt geborgd dat medewerkers geen toegang hebben tot persoonsgegevens die niet noodzakelijk zijn voor het doeleinde waarvoor zij worden verwerkt. In dat kader wijst de AP erop dat Menzis bijvoorbeeld geen logbestanden bijhoudt over de toegang tot persoonsgegevens, waaronder bijzondere persoonsgegevens.
- Het voorgaande leidt tot de conclusie dat Menzis niet beschikt over passende technologische maatregelen als bedoeld in artikel 13 van de Wbp. De AP heeft uit onderliggende stukken die weergeven op welke wijze een marketingactie bij Menzis 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 Menzis 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 Menzis haar systeem op zodanige wijze in te richten dat ongeautoriseerde toegang tot persoonsgegevens wordt voorkomen.

Zij dient daartoe in ieder geval:

1. De autorisatiematrix en bijbehorende documenten waarin zij de logische toegangsbeveiliging van haar van systemen heeft vastgelegd, dienen te worden aangepast. Deze documenten dienen zodanig te worden aangepast of opnieuw opgesteld dat hieruit duidelijk volgt welke toegangsrechten medewerkers hebben. De autorisatiematrix dient een inzichtelijk overzicht te bieden van de autorisaties en raadpleegrollen die bij een functie of rol horen door middel van onder meer een eenduidig gebruik van terminologie. Hierbij dient Menzis vast te leggen voor welke functie of rol het verwerken van persoonsgegevens betreffende de gezondheid noodzakelijk is en voor welk doeleinde en dit document indien nodig aan herziene bedrijfsinzichten aan te passen. Voorts dienen de autorisaties van medewerkers van Menzis daarmee blijvend feitelijk in overeenstemming te worden gebracht.
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. Tevens betekent dit dat de autorisaties periodiek dienen te worden gecontroleerd en onverwijld aangepast wanneer uit een controle blijkt dat een medewerker ten onrechte is geautoriseerd om inzage te hebben tot persoonsgegevens, waaronder persoonsgegevens betreffende de gezondheid.
3. Menzis 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 Menzis 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 Menzis 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 Menzis 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 Menzis, 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 Menzis niet vóór het einde van de onder 0 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 Menzis 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 Menzis, 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 Menzis 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 Menzis 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 Menzis 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 Menzis 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 marketingmedewerkers van Menzis feitelijk toegang hebben tot persoonsgegevens betreffende de gezondheid, terwijl door Menzis is vastgelegd dat dit niet de bedoeling is. Menzis heeft in haar reactie op het voornemen tot handhaving de juistheid van deze bevindingen erkend en verklaard zich te committeren aan het oordeel van de AP dat dit leidt tot een overtreding van artikel 13 van de Wbp. Menzis heeft verklaard dat zij zo spoedig mogelijk de nodige maatregelen wil nemen om de overtreding te beëindigen. Zij heeft daartoe de AP een planning verstrekt van de maatregelen die zij voornemens is te treffen. Deze planning komt de AP realistisch voor. De AP heeft daarom de hiervoor vermelde begunstigingstermijnen voor de onderscheiden onderdelen van de last onder dwangsom afgestemd op de planning van Menzis.

Datum
15 februari 2018

Ons kenmerk
[VERTROUWELIJK]

Ter voorlichting van partijen

19 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 naar de Functionaris voor de Gegevensbescherming van Menzis [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.