AUTORITEIT
PERSOONSGEGEVENS

Bevindingen VGZ

1. Gedragscode en privacybeleid

VGZ heeft in haar brief van 25 oktober 2017 aangegeven dat de coöperatie VGZ UA bestaat uit vijf verzekeringsentiteiten: VGZ Zorgverzekeraar N.V. (VGZ, NV Univé Zorg (Univé), IZA Zorgverzekeraar NV (IZA), IZZ Zorgverzekeraar NV (IZZ) inmiddels gewijzigd in VGZ voor de Zorg N.V., en NV Zorgverzekeraar UMC (UMC). Ook is VGZ Cares N.V. in 2017 gefuseerd met VGZ Zorgverzekeraar N.V. Voor al deze rechtspersonen hanteert VGZ hetzelfde beleid.

VGZ bericht dat zij persoonsgegevens verwerkt van (aspirant) verzekerden, verzekeringsnemers, werknemers die via hun werkgever onder een bedrijfszorgregeling vallen en cliënten die vallen onder de Wet langdurige zorg (Wlz) die via het Zorgkantoor van VGZ bediend worden.
Als verwerkingsdoeleinden vermeldt VGZ:

- Aangaan en uitvoeren van de verzekeringsovereenkomst (reguliere persoonsgegevens en persoonsgegevens betreffende de gezondheid);
- Uitvoeren van de Wlz (reguliere persoonsgegevens en persoonsgegevens betreffende de gezondheid);
- Marketingdoeleinden (reguliere persoonsgegevens);
- Informatieverstrekking (reguliere persoonsgegevens);
- Onderzoeken (reguliere persoonsgegevens en persoonsgegevens betreffende de gezondheid);
- Het waarborgen van de veiligheid en integriteit van onze sector (reguliere persoonsgegevens en strafrechtelijke gegevens);
- Het voldoen aan wettelijke verplichtingen.

VGZ geeft aan dat zij de volgende documenten hanteert bij het verwerken van persoonsgegevens:
a) de Gedragscode Verwerking Persoonsgegevens Zorgverzekeraars van Zorgverzekeraars Nederland;
b) de Uniforme Maatregelen opgesteld door ZN, in het bijzonder de Uniforme Maatregelen met betrekking tot Functionele eenheid (01), Privacy Statement (02), Informatie verstrekken aan verzekerden en verzekeringsnemer (03), Direct Marketing (04), Privacy afhandeling declaraties (06), Informatieuitwisseling zorgverzekeraars bij controle en fraudebeheersing (08), Gebruik authenticatiemiddelen bij internetapplicaties (09);
c) het Protocol Materiële Controle versie 31 oktober 2016 van ZN;
d) de Privacyregeling GGZ zoals neergelegd in artikel 3.5 van de Nadere regeling gespecialiseerde geestelijke gezondheidszorg van de Nederlandse Zorgautoriteit (NZa) (thans NR/REG-1734);
e) het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen.

VGZ hanteert tevens de volgende documenten mede in aanvulling op of ter verdere uitwerking van de Gedragscode
f) de Privacytekst en haar Privacystatement op haar website;
g) [VERTROUWELIJK]
h) [VERTROUWELIJK]
i) [VERTROUWELIJK]
j) [VERTROUWELIJK]
k) Functiebeschrijving CISPO;

l) [VERTROUWELIJK]
m) [VERTROUWELIJK]
n) [VERTROUWELIJK]
o) Standaard 04 – Logische Toegangsbeveiliging;
p) [VERTROUWELIJK]
q) Standaard 07 – Beveiliging bedrijfsvoering;
r) [VERTROUWELIJK]
s) [VERTROUWELIJK]
t) [VERTROUWELIJK]
u) [VERTROUWELIJK]
v) [VERTROUWELIJK]
w) [VERTROUWELIJK]
x) [VERTROUWELIJK]
y) [VERTROUWELIJK]
z) [VERTROUWELIJK]
aa) [VERTROUWELIJK]
bb) [VERTROUWELIJK]

VGZ geeft ten aanzien van de formele- en materiële controle aan dat zij over beleidsstukken beschikt in aanvulling op de Gedragscode Zorgverzekeraars. Zo is een interne gedragslijn opgesteld, alsook een overzicht van veel gestelde vragen. [VERTROUWELIJK]
VGZ geeft aan dat zij transparant is over de wijze waarop zij de controles uitvoert en hierover informatie op haar website heeft gepubliceerd:
https://www.vgz.nl/privacy
https://www.vgz.nl/privacy/wetten-en-regels
https://www.vgz.nl/nieuws/medische-gegevens-inzien-mag-vgz-dat
[VERTROUWELIJK]

[VERTROUWELIJK] Volgt uit de rapportage dat zich een afwijking voordoet op de gedragscode of Uniforme Maatregel dan vindt een risicobeoordeling plaats waarbij de privacy impact wordt onderzocht. [VERTROUWELIJK] ook geborgd dat eventuele wijzigingen in wet- en regelgeving door de afdeling Juridische Zaken worden doorgevoerd. [VERTROUWELIJK]

[VERTROUWELIJK]

Beoordeling

Naast de Gedragscode Zorgverzekeraars en de Uniforme Maatregelen van Zorgverzekeraars Nederland (ZN) hanteert VGZ diverse eigen beleidsdocumenten, werkprocessen en werkinstructies. Deze zijn aan de AP overgelegd.
Voorts stelt de AP vast dat het privacybeleid en de wijze waarop persoonsgegevens worden verwerkt periodiek getoetst worden door middel van [VERTROUWELIJK] Uit de overgelegde stukken is verder op te maken dat VGZ rekening houdt met wijzigingen in wet- en regelgeving en relevante jurisprudentie.

Voorts maakt de AP uit de documenten op dat VGZ aandacht besteedt aan awareness ten aanzien van de geldende privacywetgeving. [VERTROUWELIJK]

Gelet op het voorgaande betekent de enkele omstandigheid dat VGZ op haar website vermeldt dat zij

toepassing geeft aan de gedragscode, die inmiddels is afgekeurd, niet reeds dat VGZ handelt in strijd met de Wbp.

2. Digitale declaratie zonder diagnose-informatie

VGZ brengt naar voren dat declaraties met daarop persoonsgegevens, waaronder persoonsgegevens betreffende de gezondheid, door medewerkers van VGZ worden verwerkt die werkzaam zijn bij het [VERTROUWELIJK]. Het gaat hierbij om medewerkers met [VERTROUWELIJK] die deze persoonsgegevens verwerken voor het doel uitkering van gedeclareerde tegoeden. Bij deze werkzaamheden wordt gewerkt conform Uniforme Maatregel 03 Informatie verstrekken aan verzekerden en verzekeringsnemer. Daarnaast zijn vanuit hun functie ook medewerkers van de [VERTROUWELIJK] gemachtigd om inzicht te hebben in persoonsgegevens betreffende de gezondheid om de Zorgverzekeringswet (Zvw) te kunnen uitvoeren.

Wat betreft de privacyregeling heeft VGZ het volgende naar voren gebracht. Uit het onderzoek van de NZa uit 2016 naar de wijze waarop zorgverzekeraars de privacyregeling toepassen, volgt dat de die regeling door VGZ correct wordt uitgevoerd, zo brengt VGZ naar voren. VGZ heeft aangegeven dat zij hierbij mede gebruik maakt van de Uniforme Maatregel privacy afhandeling declaraties (06) van ZN.

VGZ geeft voorts aan dat zij na het onderzoek van de NZa in 2016 naar de uitvoering van de privacyregeling geen aanpassingen heeft doorgevoerd ten aanzien van de uitvoering van deze regeling omdat uit het onderzoek bleek dat VGZ adequaat invulling gaf aan de privacyregeling. Voor zover de NZa aanbevelingen inzake controles heeft gedaan, heeft VGZ op eigen initiatief ervoor gekozen [VERTROUWELIJK]. VGZ heeft ter toelichting de [VERTROUWELIJK] en het NZa rapport met bevindingen overgelegd. Tevens heeft VGZ de aanbevelingen van de NZa opgevolgd door blijvend aandacht te besteden aan het volgen van [VERTROUWELIJK]. VGZ heeft hieraan een toevoeging gedaan door een periodieke beoordeling op te nemen in de [VERTROUWELIJK]. Hierin is tevens de aanbeveling opgenomen om het afwijken van het advies van de medisch adviseur te motiveren. Voorts heeft VGZ de aanbeveling van de NZa opgevolgd dat medisch adviseurs die betrokken zijn bij inkoop van een bepaalde zorgaanbieder, niet ook betrokken zijn bij controles bij die zorgaanbieder en dit vast te leggen in het controleproces.

Beoordeling

Voor de wijze waarop VGZ omgaat met privacyverklaringen en het opvragen van informatie aan de verzekerden verwijst de AP naar het onderzoek van NZa uit 2016[1] dat in samenspraak met de AP is uitgevoerd. In dat onderzoek heeft de NZa geconcludeerd dat de mate van naleving van de privacyregeling van de NZa over het algemeen goed is.

De AP onderschrijft de bevindingen zoals vastgelegd in dat onderzoek. Tijdens het onderhavige onderzoek van de AP is verder niet gebleken van wijzigingen in het beleid of werkwijze van VGZ die tot een nader onderzoek op dit punt dienen te leiden.

3. Doelbinding

-marketing

[1] https://www.nza.nl/1048076/1048181/Rapport_Zorgverzekeraars_controles_en_privacyvoorschriften_september_2016.pdf

VGZ geeft aan dat zij geen persoonsgegevens betreffende de gezondheid verwerkt voor marketingdoeleinden. Voor dit doeleinde gebruikt zij uitsluitend reguliere persoonsgegevens. Hierover wordt transparant gecommuniceerd in het privacystatement op de website van VGZ. Verzekerden kunnen zich altijd beroepen op het recht van verzet. Verzekerden die zich hierop hebben beroepen worden uitgesloten van een marketingactie.
VGZ heeft een voorbeeld overgelegd van een aantal documenten waaruit haar werkwijze ten aanzien van een marketingplan blijkt: [VERTROUWELIJK] resultaat van een voorbeeldcampagne.

VGZ heeft toegelicht dat het marketingproces bestaat uit de volgende stappen: [VERTROUWELIJK].

-uitzondering op doelbinding
Voor zover in de Gedragscode zorgverzekeraars de mogelijkheid bestaat om een uitzondering op het doelbindingsbeginsel te maken, geeft VGZ aan dat zij in uitzonderingsgevallen gebruik maakt van de mogelijkheid die is neergelegd in artikel 3.13 van de Gedragscode.

VGZ heeft in haar brief van 12 december 2017 aan de AP toegelicht dat zij gebruik maakt van de uitzondering van artikel 3.13 van de Gedragscode voor het doen van aangifte van bijvoorbeeld fraude of bij vordering van gegevens door politie, justitie en de Belastingdienst in het geval van fraude. Tevens heeft VGZ aangegeven hierbij gebruik te maken van de Uniforme Maatregel 08 - Uitwisseling persoonsgegevens tussen zorgverzekeraars bij diverse vormen van controle en fraudebeheersing - in aanvulling op de Gedragscode. VGZ licht toe dat in het dossier van betrokkene wordt vastgelegd dat persoonsgegevens worden gedeeld, met wie, wat hiervan het doel is en wat de overwegingen hierbij zijn geweest. [VERTROUWELIJK]. Tevens worden de richtlijnen van ZN en het Verbond van Verzekeraars gehanteerd, zoals 'handvatten aangifte Loket Verzekeringsfraude'. [VERTROUWELIJK]
De AP heeft inzage gehad in de werkinstructies waarnaar VGZ verwijst.

Beoordeling
De AP constateert dat geen sprake is van het ter zijde stellen van het doelbindingsvereiste voor willekeurige doeleinden. Zo is niet gebleken van het verwerken van persoonsgegevens betreffende de gezondheid ten behoeve van marketingdoeleinden. Op grond van de overgelegde documenten heeft VGZ aannemelijk gemaakt dat zowel de marketinguitingen, als het interne beoordelingsproces dat daaraan vooraf gaat, niet zijn gebaseerd op persoonsgegevens betreffende de gezondheid.

Desgevraagd heeft VGZ te kennen gegeven dat zij net als de andere zorgverzekeraars gebruik maakt van de uitzondering als bedoeld in artikel 3.13 van de Gedragscode of artikel 43 van de Wbp bij aangifte van of informatieverzoeken inzake fraudegevallen waarbij informatie verstrekt dient te worden aan politie, justitie en/of de Belastingdienst. Het uitgangspunt van VGZ is dat in beginsel ook in die gevallen geen persoonsgegevens betreffende de gezondheid worden verstrekt. Dit gebeurt alleen als deze expliciet worden gevorderd, bijvoorbeeld in de gevallen waarin de artikelen 126nf en 126uf van het Wetboek van Strafvordering voorzien. Deze verstrekkingen worden behandeld door de [VERTROUWELIJK] en mogen uitsluitend plaatsvinden na instemming door een medisch adviseur. Deze verstrekkingen en de instemming van de medisch adviseur worden schriftelijk vastgelegd in het dossier van de betrokkene. Hierbij wordt meer specifiek vastgelegd op basis van welke wettelijke grondslag, aan wie en welke

persoonsgegevens, waaronder persoonsgegevens betreffende de gezondheid, worden verstrekt, waarom dit noodzakelijk is en welke weging hierbij heeft plaatsgevonden.

Voor de verstrekking van persoonsgegevens (betreffende de gezondheid) aan politie, justitie, de Belastingdienst en wettelijke toezichthouders is een grondslag aanwezig, namelijk een wettelijke verplichting, als bedoeld in artikel 8, aanhef en onder c, van de Wbp. Deze verstrekkingen zijn in overeenstemming met artikel 43, aanhef en onder b, c, en d, van de Wbp. In het geval van een dergelijke verstrekking wordt gebruik gemaakt van de Uniforme Maatregel 8 van ZN, in aanvulling op artikel 3.13 van de Gedragscode zorgverzekeraars, alsmede de richtlijn 'handvatten aangifte Loket Verzekeringsfraude' en interne werkinstructies. Deze documenten bevatten een voldoende specifieke uitwerking van dit artikel voor zorgverzekeraars. Dit betekent dat VGZ gebruik maakt van aanvullend beleid waarin artikel 3.13 van de Gedragscode is uitgewerkt ten behoeve van zorgverzekeraars en sprake is van een rechtmatige uitzondering.

Uit de onderliggende informatie is niet gebleken van enige onrechtmatige verstrekkingen door VGZ aan derden, nu sprake is van een wettelijke grondslag en in beginsel uitsluitend reguliere persoonsgegevens worden verstrekt en geen persoonsgegevens betreffende de gezondheid. Worden persoonsgegevens betreffende de gezondheid verstrekt, dan geschiedt dit eerst nadat de medisch adviseur heeft bepaald of er een grondslag is voor deze verstrekking en het verstrekken van deze gegevens noodzakelijk is. De AP heeft bovendien geen aanwijzingen of signalen ontvangen die aanknopingspunten bieden voor een andere conclusie. Derhalve is niet gebleken dat VGZ voor dit doeleinde meer persoonsgegevens verstrekt dan noodzakelijk is en evenmin is gebleken dat VGZ persoonsgegevens verstrekt zonder dat daarvoor een grondslag zou bestaan.

4. Ongeautoriseerde toegang tot persoonsgegevens

[VERTROUWELIJK]

Wat betreft het beveiligingsbeleid van VGZ is het volgende van belang. [VERTROUWELIJK]

Wat betreft de systemen waarmee VGZ werkt, is het volgende van belang. VGZ maakt gebruik van verschillende systemen en applicaties voor hun bedrijfsprocessen. VGZ heeft een applicatieoverzicht aangeleverd met een omschrijving van verschillende applicaties waarin persoonsgegevens worden verwerkt. [VERTROUWELIJK]

Wat betreft het autorisatiebeleid is het volgende van belang. [VERTROUWELIJK]

Bij het onderzoek ter plaatse heeft VGZ verklaard dat [VERTROUWELIJK] een zogeheten certificeringsronde wordt gehouden, waarbij de verantwoordelijke manager alle verleende autorisaties controleert en accordeert.

[VERTROUWELIJK]

Wat betreft de logging heeft VGZ het volgende naar voren gebracht. [VERTROUWELIJK]

Beoordeling

-autorisatiebeleid

[VERTROUWELIJK] De AP doet evenwel aan VGZ de **aanbeveling** 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.

-logging

In de antwoorden van 25 oktober 2017 stelt VGZ: [VERTROUWELIJK]

-conclusie

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. [VERTROUWELIJK]
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.

5. Bewerkers

VGZ heeft aangegeven bij [VERTROUWELIJK] gebruik te maken van [VERTROUWELIJK] externe bewerkers voor het verwerken van persoonsgegevens betreffende de gezondheid. Het gaat om verschillende organisaties, variërend van callcenters en incassobedrijven, tot ICT-organisaties en organisaties die zich bezighouden met het scannen van declaraties en het printen, grafisch afwerken, couverteren en verzenden van overig drukwerk. Een lijst met bewerkers is overgelegd.

In haar brief geeft VGZ aan dat borging van wet- en regelgeving inzake persoonsgegevens in zijn algemeenheid inhoudt dat [VERTROUWELIJK] bij de projectstart betrokken is, waarbij het inkoopproces wordt doorlopen. [VERTROUWELIJK] dat er (mogelijk) sprake is van verwerking van persoonsgegevens, dan neemt [VERTROUWELIJK] voor het opstellen van de bewerkersovereenkomst. Een volledig ingevulde bewerkersovereenkomst wordt aan de [VERTROUWELIJK] aangeleverd die deze toevoegt aan de

hoofdovereenkomst.
[VERTROUWELIJK] getoetst of een bewerkersovereenkomst nog actueel is. [VERTROUWELIJK] draagt zorg voor het aanpassen van het beleid, specifieke instructies of implementatie van aanvullend/gewijzigd beleid e.d.

VGZ heeft haar standaard-bewerkersovereenkomst meegezonden. Hierin zijn de verplichtingen voor de bewerkers en eventuele sub-bewerkers expliciet uitgewerkt. Het gaat onder meer om de naleving van de Wbp, de eisen van strikte doelbinding, geheimhouding, beveiliging en controle, meldplicht datalekken, het inschakelen van een sub-bewerker uitsluitend met schriftelijke toestemming van VGZ en tijdige vernietiging van persoonsgegevens.

Beoordeling

De AP heeft kennis genomen van de hiervoor vermelde stukken en standaardteksten- en contracten. Hierin heeft VGZ een nadere invulling gegeven aan de Gedragscode Zorgverzekeraars. Verder blijkt hieruit dat bewerkers zich ook dienen te houden aan de bijzondere eisen die gelden uit de Wbp ten aanzien van de verwerking van persoonsgegevens betreffende de gezondheid. Zo zijn bewerkers verplicht om technologische en organisatorische maatregelen te treffen ter beveiliging van persoonsgegevens betreffende de gezondheid en zich ook overigens aan de Wbp te houden waaronder de meldplicht datalekken uit artikel 34a van de Wbp. Uit de standaardovereenkomst en standaardtekst volgt dat VGZ toeziet op de correcte naleving van de Wbp. Bewerkers worden zo expliciet gewezen op de bijzondere eisen die gelden uit de Wbp ten aanzien van de verwerking van persoonsgegevens betreffende de gezondheid en de geheimhouding. [VERTROUWELIJK] De AP maakt hieruit op dat is voldaan aan de verplichtingen die zijn neergelegd in artikel 14 van de Wbp in samenhang met de artikelen 12, 13 en 34a van de Wbp.

6. Medisch beroepsgeheim

VGZ heeft verschillende functionele eenheden (FE's) ingericht. Medewerkers die werken binnen een FE vallen onder de functionele verantwoordelijkheid van medisch adviseur. Bij VGZ zijn [VERTROUWELIJK] medisch adviseurs in dienst, die allen geregistreerd zijn volgens de Wet BIG. [VERTROUWELIJK] De medisch adviseur die aan het hoofd staat van een FE is verantwoordelijk voor het nakomen van de privacyregels en de overige interne randvoorwaarden voor het omgaan met medische gegevens. De medisch adviseur heeft een functionele verantwoordelijkheid voor het nakomen van de interne gedragsregels door een FE. De medisch adviseur bewaakt dat de FE functioneert zoals bedoeld en dat de 'privacyawareness' van de medewerkers en de managers op voldoende niveau is. [VERTROUWELIJK]

[VERTROUWELIJK]

Wat betreft de geheimhoudingsovereenkomsten heeft VGZ het volgende naar voren gebracht. Verwerking van persoonsgegevens over iemands gezondheid vindt binnen VGZ plaats onder functionele aansturing van een medisch adviseur. [VERTROUWELIJK]

Beoordeling

-geheimhouding
De AP stelt in de eerste plaats vast dat de medisch adviseurs die de FE's aansturen allen arts zijn en zijn geregistreerd volgens de Wet BIG (BIG-geregistreerd). Daarmee rust op hen een geheimhoudingsplicht

rust uit hoofde van beroep.[2]

Op alle medewerkers van VGZ rust een geheimhoudingsplicht uit hoofde van een (geheimhoudings)overeenkomst. [VERTROUWELIJK] Op basis van de toegezonden stukken overweegt de AP dat er organisatorische maatregelen zijn getroffen om te waarborgen dat medewerkers die persoonsgegevens betreffende iemands gezondheid verwerken daadwerkelijk geheimhoudingsverklaringen ondertekenen en dat daarop voldoende sturing plaatsvindt.

Gelet hierop komt de AP tot de conclusie dat VGZ voldoet aan het bepaalde in artikel 21, eerste lid, aanhef en onder b, van de Wbp, in samenhang gelezen met het tweede lid, nu de persoonsgegevens betreffende de gezondheid worden verwerkt door personen die uit hoofde van hun beroep of een krachtens een overeenkomst onderworpen zijn aan een geheimhoudingsplicht.

-noodzakelijkheidsvereiste
VGZ heeft aan de rol van de medisch adviseur invulling gegeven door taken te beleggen in zogenaamde FE's waarin persoonsgegevens betreffende de gezondheid worden verwerkt onder verantwoordelijkheid van een medisch adviseur. Bij de inrichting van de FE's heeft VGZ rekening gehouden met de Uniforme Maatregelen inzake de Functionele Eenheid van ZN en het Kader Functionele Eenheid Controles. De AP stelt op basis van de stukken vast dat de medisch adviseur een duidelijke rol heeft in het kader van de omgang met gezondheidsgegevens binnen zijn/haar bedrijfsonderdeel. [VERTROUWELIJK]

Gelet op het voorgaande komt de AP tot de conclusie dat VGZ met de door haar gekozen invulling van de rol van de medisch adviseur voldoende heeft gewaarborgd dat de beoordeling of interpretatie van de noodzaak tot de verwerking van persoonsgegevens betreffende de gezondheid in overeenstemming met de Wbp en de Zvw plaatsvindt door iemand met voldoende (medische) kennis van zaken.

-detailcontrole
De vraag of zorgverzekeraars in overeenstemming met artikel 7.8 van de Rzv handelen, maakt onderdeel uit van het onderzoek dat de NZa in 2016 – in samenspraak met de AP – heeft verricht. De NZa heeft op basis van dat onderzoek geconcludeerd dat geen van de zorgverzekeraars op dit punt een overtreding begaan. De AP heeft tijdens het onderhavige onderzoek bij VGZ geen aanknopingspunten gevonden om aan de bevindingen van de NZa op dit punt te twijfelen.

-conclusie
Gelet op het voorgaande komt de AP tot de conclusie dat VGZ op het punt van het medisch beroepsgeheim niet handelt in strijd met de Wbp.

[2] Op grond van artikel 88 van de Wet BIG is een ieder die een beroep op het gebied van de individuele gezondheidszorg uitoefen, verplicht tot geheimhouding wat hem bij de uitoefening van zijn beroep is toevertrouwd. Daarnaast geldt tevens een medische zwijgplicht, zoals neergelegd in artikel 7:457 van het Burgerlijk Wetboek (BW), ook wel aangeduid als de Wet inzake de geneeskundige behandelingsovereenkomst.

Conclusies

Hieronder is per onderdeel een conclusie opgenomen.

Gedragscode en privacybeleid

Gelet op het gebruik van de Uniforme Maatregelen en het eigen privacybeleid van VGZ is de AP van oordeel dat het enkele feit dat VGZ op haar website vermeldt dat zij toepassing geeft aan de gedragscode, die inmiddels is afgekeurd, niet reeds dat VGZ handelt in strijd met de Wbp.

Digitale declaratie zonder diagnose-informatie

De AP onderschrijft de bevindingen zoals vastgelegd in het aangehaalde onderzoek van de NZa. Tijdens het onderhavige onderzoek van de AP is verder niet gebleken van wijzigingen in het beleid of werkwijze van VGZ die tot een nader onderzoek op dit punt dienen te leiden.

Doelbinding

De AP is niet gebleken van enige onrechtmatige verstrekkingen door VGZ aan derden, nu sprake is van een wettelijke grondslag en in beginsel uitsluitend reguliere persoonsgegevens worden verstrekt en geen persoonsgegevens betreffende de gezondheid. Worden persoonsgegevens betreffende de gezondheid verstrekt, dan geschiedt dit eerst nadat de medisch adviseur heeft bepaald of er een grondslag is voor deze verstrekking en het verstrekken van deze gegevens noodzakelijk is. De AP heeft bovendien geen aanwijzingen of signalen ontvangen die aanknopingspunten bieden voor een andere conclusie. Derhalve is niet gebleken dat VGZ voor dit doeleinde meer persoonsgegevens verstrekt dan noodzakelijk is en evenmin is gebleken dat VGZ persoonsgegevens verstrekt zonder dat daarvoor een grondslag zou bestaan.

Ongeautoriseerde toegang tot persoonsgegevens

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. [VERTROUWELIJK]
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.

Bewerkers

Uit de standaardovereenkomst en standaardtekst volgt dat VGZ toeziet op de correcte naleving van de Wbp op dit punt. Bewerkers worden zo expliciet gewezen op de bijzondere eisen die gelden uit de Wbp ten aanzien van de verwerking van persoonsgegevens betreffende de gezondheid en de geheimhouding. [VERTROUWELIJK] De AP maakt hieruit op dat is voldaan aan de verplichtingen die zijn neergelegd in artikel 14 van de Wbp in samenhang met de artikelen 12, 13 en 34a van de Wbp.

Medisch beroepsgeheim

De AP komt tot de conclusie dat VGZ op het punt van het medisch beroepsgeheim niet handelt in strijd met de Wbp.
De AP concludeert namelijk dat persoonsgegevens betreffende de gezondheid binnen VGZ worden verwerkt door personen op wie een geheimhoudingsplicht rust uit hoofde van een beroep (arts) alsmede uit een overeenkomst (medewerkers VGZ). Gelet hierop komt de AP tot de conclusie dat VGZ voldoet aan het bepaalde in artikel 21, eerste lid, aanhef en onder b, van de Wbp, in samenhang gelezen met het tweede lid.
Voorts komt de AP tot de conclusie dat VGZ met de door haar gekozen invulling van de rol van de medisch adviseur voldoende heeft gewaarborgd dat de beoordeling of interpretatie van de noodzaak tot de verwerking van persoonsgegevens betreffende de gezondheid in overeenstemming met de Wbp en de Zvw plaatsvindt door iemand met voldoende (medische) kennis van zaken.
De vraag of zorgverzekeraars ten slotte in overeenstemming met artikel 7.8 van de Rzv handelen, maakt ten slotte onderdeel uit van het onderzoek dat de NZa in 2016 – in samenspraak met de AP – heeft verricht. De NZa heeft op basis van dat onderzoek geconcludeerd dat geen van de zorgverzekeraars op dit punt een overtreding begaan. De AP heeft tijdens het onderhavige onderzoek bij VGZ geen aanknopingspunten gevonden om aan de bevindingen van de NZa op dit punt te twijfelen.