AUTORITEIT
PERSOONSGEGEVENS

Bevindingen Menzis

1. Gedragscode en privacybeleid

Tot de Menzis Groep behoren de volgende risicodragers: Menzis Zorgverzekeraar N.V., Menzis N.V. en Anderzorg N.V. Daarbij hoort ook uitvoering van de Wet langdurige zorg (Wlz) door Stichting Zorgkantoor Menzis, voor zover het verzekerden van Menzis betreft. De informatie die Menzis heeft verstrekt, gaat op voor alle genoemde rechtspersonen.

Menzis geeft aan dat zij persoonsgegevens verwerkt van verzekerden op grond van de Zorgverzekeringswet (Zvw), de Wlz en ten aanzien van personen die een (aanvullende) zorgverzekering hebben gesloten. Verwerking geschiedt voor de doeleinden: uitvoering van de verzekeringsovereenkomst, voor commerciële doeleinden (gerechtvaardigd belang) en vanwege wettelijke verplichtingen. Voor zover persoonsgegevens betreffende de gezondheid worden verwerkt, geschiedt dit in het kader van de uitvoering van de verzekering, zo brengt Menzis naar voren.
Menzis verwerkt voorts persoonsgegevens van zorgaanbieders, werknemers, potentiële klanten en personen die zich hebben aangemeld voor het SamenGezond programma.

Menzis 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.

Menzis hanteert tevens de volgende documenten, mede in aanvulling op of ter verdere uitwerking van de Gedragscode:
f) Menzis beleid voor bescherming persoonsgegevens;
g) richtlijn bewaren en vernietigen van gegevens;
h) richtlijn gegevens verstrekken aan derden;
i) richtlijn Privacy organisatie;
j) Procedure inzage- en correctierecht;
k) Procedure recht van verzet;
l) Procedure melding gegevensverwerking;
m) Procedure verkeerd geadresseerde medische dossiers;
n) Modelovereenkomst voor uitleveren van persoonsgegevens;
o) naleving van de Gedragscode Verwerking Persoonsgegevens Zorgverzekeraars;
p) Wetenschappelijk statistisch onderzoek;
q) Protocol meldplicht datalekken;
r) Beleid voor Informatiebeveiliging;

s) Reglement inrichting Functionele Eenheid;
t) Geheimhoudingsverklaringen (tekst arbeidsovereenkomst, functionele eenheden, etc.).
u) Toelichting activiteiten Compliance Functie;
v) Thematisch kader compliance 2017 versie E&Y;
w) Voorlegger actualiseren beleid, richtlijnen en procedures privacy;
x) Beleidsrichtlijn logische toegangsbeveiliging;
y)Menzis beleid voor functiescheiding 3.0;
z) Toestemmingsverklaring SamenGezond;
aa) Werkdocument contractgids;
bb) SCB Privacy en beveiligingsmaatregelen;
cc) Artikel 15 AIV Privacy en Informatiebeveiliging.

Menzis heeft toegelicht dat zij een compliance control framework heeft, aan de hand waarvan zij toetst of op de juiste wijze uitvoering wordt gegeven aan privacywetgeving en beleid. Dit systeem bestaat uit een gedetailleerd exceloverzicht met een lijst van alle te toetsen onderdelen uit diverse zogeheten toezichtgebieden. Zo zijn de bepalingen uit geldende en toekomstige privacywet- en regelgeving vermeld en de daarbij te toetsen norm, aan welke criteria voldaan dient te zijn om te kunnen concluderen dat aan de norm is voldaan en op welke manier daarvoor bewijs moet worden aangeleverd. De bedrijfsonderdelen van Menzis worden periodiek integraal doorgelicht op de toepassing van de beheersmaatregelen uit het compliance control framework. Dit heeft mede tot doel het privacybeleid van Menzis aan te passen aan geldende wet- en regelgeving en andere relevante ontwikkelingen, waaronder jurisprudentie.

De Functionaris voor de Gegevensbescherming en de [VERTROUWELIJK] hanteren een risicogestuurde en thematische aanpak om controle te houden op de borging van privacy. De gehele organisatie wordt elke [VERTROUWELIJK] bevraagd ten aanzien van de geselecteerde risico's en thema's. Alle clusters (totaal [VERTROUWELIJK]) binnen Menzis die te maken hebben met verwerking van persoonsgegevens, worden hierbij betrokken. Dit leidt tot een rapportage met een score of voldaan wordt aan deze onderdelen. Het laatste onderzoek dateert uit [VERTROUWELIJK] en heeft tot opvolging van diverse aandachtspunten in [VERTROUWELIJK] geleid.

Met het oog op de komst van de Algemene Verordening Gegevensbescherming (AVG) per 25 mei 2018 heeft Menzis in samenwerking met [VERTROUWELIJK] een nieuw control framework opgesteld, op basis waarvan de organisatie in het vierde kwartaal van 2017 zal worden getoetst op compliance. Vooruitlopend op de AVG worden reeds Privacy Impact Assessments verricht voor de belangrijkste bedrijfsfuncties, waaronder de bedrijfsfuncties [VERTROUWELIJK]

Het uitgangspunt van Menzis is dat het gebruik van persoonsgegevens betreffende de gezondheid alleen is toegestaan voor medewerkers die vanuit hun functie en werkzaamheden deze gegevens nodig hebben en indien wordt voldaan aan de noodzakelijkheidstoets (proportionaliteits- en subsidiariteitseisen). Dit uitgangspunt is ingebed in de cultuur van Menzis door middel van haar privacybeleid, awareness programma's en het opleidingsprogramma van nieuwe medewerkers (e-learning) en het doorlopende opleidingsprogramma van bestaande medewerkers. Alle medewerkers zijn verplicht om een geheimhoudingsverklaring te ondertekenen en deze na te leven. Leidinggevenden benadrukken dit bij herhaling. Awareness voor naleving van geldende wet- en regelgeving die ziet op de bescherming van persoonsgegevens wordt zoveel mogelijk gestimuleerd. Sinds [VERTROUWELIJK] worden er rondom dit thema jaarlijks activiteiten georganiseerd, zoals een 'Week voor de privacy', waarin alle medewerkers erop

worden gewezen wat er op dit gebied wel en niet is toegestaan. Verder worden wijzigingen in het beleid besproken. Afgelopen jaar bestond deze week onder meer uit het naspelen van concrete incidenten door acteurs, gevolgd door een uitleg over de toegestane handelswijze. Verder bestond deze week uit het geven van informatie, en konden er vragen worden gesteld over privacy. Menzis heeft verder met behulp van mystery guests getoetst of in de praktijk sprake is van (mogelijke) niet naleving van de normen. Dit is verder getest met behulp van een namaak phishing e-mail. Ook de invoering van de meldplicht datalekken en de komst van de AVG spelen in dit kader een relevante rol. Managers zijn er verantwoordelijk voor dat hun medewerkers blijvend worden geïnformeerd over belangrijke ontwikkelingen, alsook dat daarop in concrete dossiers wordt getoetst.

Beoordeling

De Autoriteit Persoonsgegevens (AP) concludeert dat Menzis niet uitsluitend gebruik maakt van de Gedragscode, maar daarnaast de Uniforme Maatregelen van Zorgverzekeraars Nederland (ZN) hanteert, alsmede diverse eigen beleidsdocumenten, werkprocessen en werkinstructies. De AP heeft kennis genomen van alle overgelegde stukken. Deze documenten zijn nader uitgewerkt in concrete werkprocessen en werkinstructies die zijn toegespitst op de werkzaamheden van Menzis als zorgverzekeraar. De AP stelt verder vast dat Menzis heeft voorzien in processen ten behoeve van de controle op de naleving van haar privacybeleid.

Voorts stelt de AP vast dat Menzis zorgdraagt voor aanpassing van het privacybeleid aan wijzigingen in wet- en regelgeving en jurisprudentie.

Ten slotte maakt de AP uit de interviews en aangeleverde documenten op dat Menzis aandacht besteedt aan het correct naleven van geldende wet- en regelgeving die ziet op de bescherming van persoonsgegevens. Onder meer door e-learningprogramma's en themaweken worden de medewerkers van Menzis zo veel mogelijk bewust gemaakt van de manier waarop met persoonsgegevens moet worden omgegaan. De AP maakt uit deze activiteiten op dat Menzis belang hecht aan correcte naleving van de geldende wet- en regelgeving alsmede van haar privacybeleid zoals dat is vastgelegd in aanvullende documenten , werkprocessen en werkinstructies.

Gelet op het voorgaande betekent de enkele omstandigheid dat Menzis op haar website vermeldt dat zij toepassing geeft aan de gedragscode – die inmiddels is afgekeurd, niet reeds dat Menzis handelt in strijd met de Wet bescherming persoonsgegevens (Wbp).

2. Digitale declaratie zonder diagnose-informatie

Naar aanleiding van uitspraak van het CBB dat zorgverzekeraars dienen te voorzien in een privacyregeling op basis waarvan GGZ-patiënten zonder vermelding van diagnose informatie moeten kunnen declareren,[1] heeft de NZa in maart 2012 voorzien in een regeling. In aansluiting hierop heeft Menzis in haar verzekeringsvoorwaarden sinds 2014 de volgende tekst standaard opgenomen:
! Let op
Indien u geen vermelding van de diagnosecode op de declaratie wenst, maar de declaratie toch voor vergoeding in aanmerking wilt laten komen, is voorafgaand of uiterlijk bij de eerste declaratie een verklaring nodig. U dient samen met uw behandelaar een verklaring te ondertekenen en naar Menzis op te sturen. Deze verklaring is te vinden op

[1] CBB 2 augustus 2010, ECLI:NL:CBB:2010:BN3056.

www.menzis.nl/vergoedingen.

Tevens heeft Menzis toegelicht dat zij naar aanleiding van het onderzoek van de NZa in 2016 door middel van het invoeren van standaardbrieven ervoor zorgdraagt dat in geval een verzekerde gebruik maakt van een privacyverklaring, niet langer wordt gevraagd naar de integrale verwijsbrief of behandelplan.

Beoordeling

Voor de wijze waarop Menzis omgaat met privacyverklaringen en het opvragen van informatie aan de verzekerden verwijst de AP naar het onderzoek van NZa uit 2016[2] 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 Menzis die tot een nader onderzoek op dit punt dienen te leiden.

3. Doelbinding

-marketing

Menzis geeft aan dat zij geen persoonsgegevens betreffende de gezondheid verwerkt voor marketingdoeleinden. Een uitzondering hierop is het gezondheidsprogramma “SamenGezond”. In het kader van dit programma worden persoonsgegevens betreffende de gezondheid uitsluitend met uitdrukkelijke toestemming van de deelnemer verwerkt. Trekt de deelnemer zijn toestemming in, dan wordt het programma beëindigd.

Menzis heeft uiteengezet hoe een reguliere marketingactie intern tot stand komt. [VERTROUWELIJK] Nadat een conceptactie binnen de [VERTROUWELIJK] is goedgekeurd, wordt deze vervolgens voorgelegd aan onder meer de [VERTROUWELIJK]. Deze afdelingen beoordelen onder andere of voor de uitvoering van de marketingactie persoonsgegevens worden verwerkt, of er geen gebruik wordt gemaakt van persoonsgegevens betreffende de gezondheid, alsook of de (reguliere) persoonsgegevens die worden verwerkt noodzakelijk zijn voor het beoogde doeleinde. Uit de overgelegde documenten volgt dat marketingmedewerkers geadresseerden van een eventuele marketingactie uitsluitend selecteren op basis van reguliere persoonsgegevens zoals naam, adres, e-mail- en telefoongegevens, aanduiding man of vrouw en geboortedatum of verzekeringsproduct. Dit is bevestigd tijdens de interviews. Een voorbeeld van een marketingactie is overgelegd in de vorm van een nieuwsbrief. Het voorbeeld geeft geen aanwijzingen dat de ontvanger ervan is geselecteerd op basis van persoonsgegevens betreffende de gezondheid.

-uitzondering op doelbinding

Voor zover in de Gedragscode de mogelijkheid bestaat om een uitzondering op het doelbindingsbeginsel te maken, geeft Menzis aan dat zij niet actief gebruik maakt van deze mogelijkheid die is neergelegd in artikel 3.13 van de Gedragscode bevat.

Menzis heeft naar voren gebracht dat zij alleen in het geval van aangifte of wanneer zij daartoe een vordering van politie of justitie, dan wel de Belastingdienst ontvangt, toepassing geeft aan artikel 3.13 van de Gedragscode en overgaat tot het verstekken van persoonsgegevens (betreffende de gezondheid). Bij het

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

verstrekken van persoonsgegevens wordt gebruik gemaakt van de Uniforme Maatregel 8 van ZN. Een verstrekking als hier aan de orde wordt altijd schriftelijk vastgelegd en betreft een beslissing die op directieniveau wordt genomen na een positief advies van de [VERTROUWELIJK]. Een lijst met vorderingen van politie, justitie of Belastingdienst over 2017 is door Menzis aan de AP overgelegd. [VERTROUWELIJK]

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 Menzis aannemelijk gemaakt dat zowel de marketinguitingen, als het interne beoordelingsproces dat daaraan vooraf gaat, niet zijn gebaseerd op persoonsgegevens betreffende de gezondheid.

De AP stelt vast dat Menzis in uitzonderlijke gevallen gebruik maakt van de mogelijkheid die is opgenomen in artikel 3.13 van de Gedragscode. Deze bepaling is nagenoeg gelijk aan artikel 43 van de Wbp.

Uitsluitend in het geval van aangifte door Menzis of vorderingen van politie, justitie en de Belastingdienst verstrekt Menzis persoonsgegevens. Het gaat dan met name om gevallen van fraude. Het uitgangspunt van Menzis 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 zijn uitsluitend mogelijk na (schriftelijke) instemming van de directie en worden schriftelijk vastgelegd

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, alsmede interne beleidsdocumenten, in aanvulling op artikel 3.13 van de Gedragscode. De Uniforme maatregel 8 bevat naar het oordeel van de AP een voldoende specifieke uitwerking van dit artikel voor zorgverzekeraars. Uit de onderliggende informatie is niet gebleken van enige onrechtmatige verstrekkingen door Menzis aan derden nu sprake is van een wettelijke grondslag en in beginsel uitsluitend reguliere persoonsgegevens worden verstrekt en geen persoonsgegevens betreffende de gezondheid. Derhalve is niet gebleken dat Menzis voor dit doeleinde meer persoonsgegevens verstrekt dan noodzakelijk is en evenmin is gebleken dat Menzis persoonsgegevens verstrekt zonder dat daarvoor een wettelijke grondslag zou bestaan. De AP heeft bovendien geen aanwijzingen of signalen ontvangen die aanknopingspunten bieden voor een andere conclusie.

4. Ongeautoriseerde toegang tot persoonsgegevens

[VERTROUWELIJK]

Beoordeling

-autorisatiebeleid algemeen
[VERTROUWELIJK]

-autorisaties medewerkers afdeling marketing
[VERTROUWELIJK]

In aanvulling hierop is het volgende van belang. Hoewel Menzis inzichtelijk heeft gemaakt dat medewerkers voortdurend worden gewezen op de wijze waarop zij met persoonsgegevens betreffende de gezondheid dienen om te gaan en dat hierop wordt gecontroleerd door hun leidinggevenden door middel van de wekelijkse dossiercontroles, is het voor Menzis niet mogelijk om te controleren of haar medewerkers zich daar in de praktijk aan houden. [VERTROUWELIJK]

Door de AP is vooralsnog niet vastgesteld dat marketingmedewerkers *daadwerkelijk* persoonsgegevens betreffende de gezondheid verwerken voor het verrichten van marketingacties. [VERTROUWELIJK]

-conclusie
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.

5. Bewerkers

Menzis heeft te kennen gegeven dat zij overeenkomsten heeft met in totaal [VERTROUWELIJK] bewerkers en hiervoor standaardteksten en -contracten hanteert waarin de bepalingen uit de Wbp en de Gedragscode verder zijn vormgegeven. De standaardteksten en -contracten die Menzis hanteert, zijn aan de AP overgelegd. Deze zijn door Menzis reeds aangepast in het licht van de AVG.

Beoordeling
De AP heeft zowel de standaardteksten- en contracten als een ingevulde versie van een bewerkersovereenkomst ontvangen. Daaruit maakt de AP op dat in die overeenkomsten is voorzien in een

vertaling van de verplichtingen die volgen uit de Wbp en de Gedragscode voor de bewerkers van Menzis en dat dit een nadere uitwerking betreft van de bepalingen uit de Gedragscode zorgverzekeraars. Zo zijn bewerkers onder andere 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 Menzis toeziet op de correcte naleving van de Wbp. Bewerkers worden zo expliciet gewezen op de bijzondere eisen die gelden op grond van de Wbp ten aanzien van de verwerking van persoonsgegevens betreffende de gezondheid. De AP concludeert op grond hiervan dat door Menzis op dit punt 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

Menzis geeft aan dat zij werkt met [VERTROUWELIJK]. Elke FE wordt aangestuurd door een medisch adviseur. [VERTROUWELIJK]

Wat betreft de geheimhouding heeft Menzis het volgende toegelicht.
FE-medewerkers zijn verplicht om bij indiensttreding een geheimhoudingsverklaring te ondertekenen. De geheimhoudingsverklaring maakt onderdeel uit van de individuele arbeidsovereenkomsten van Menzis medewerkers en ook zijn deze medewerkers op basis van de geldende collectieve arbeidsovereenkomst (cao) tot geheimhouding gehouden. Medewerkers die in een FE werken tekenen in verband met het verwerken van persoonsgegevens betreffende de gezondheid daarnaast ook nog een extra FE-geheimhoudingsverklaring. Menzis medewerkers die klantcontact hebben moeten tevens een eed of belofte afleggen waarin wordt beloofd dat zij geheim houden wat hen is toevertrouwd aan de telefoon. In aanvulling op deze maatregelen worden jaarlijks privacy awareness programma's uitgevoerd door middel van e-learning, presentaties in werkoverleggen door de Functionaris voor de Gegevensbescherming en/of de Compliance officer, bezoeken door een mysterie guest en videoboodschappen van de CEO.

Over de rol van de medisch adviseur heeft Menzis het volgende toegelicht.
De medisch adviseur bepaalt in grote lijnen of en welke persoonsgegevens betreffende de gezondheid noodzakelijk zijn en bijvoorbeeld moeten worden opgevraagd bij een zorgaanbieder. Zoveel als mogelijk wordt gewerkt met standaardinstructies en werkprocessen waarin de bescherming van persoonsgegevens zijn ingebed. Deze instructies en werkprocessen zijn mede door de medisch adviseur opgesteld en worden ten minste [VERTROUWELIJK] geëvalueerd en bijgesteld. Zo nodig gebeurt dat eerder.

Menzis heeft tijdens het interview verder toegelicht dat wanneer daarom wordt verzocht, ook het uitvoeren van een detailcontrole op dossierniveau bij een zorgaanbieder ter plaatse tot de werkzaamheden van een medisch adviseur behoort.

De (team)manager(s) binnen een FE is respectievelijk zijn primair verantwoordelijk voor het proces op zijn respectievelijk hun afdeling, terwijl de medisch adviseur aangeeft aan welke organisatorische en operationele specificaties het proces moet voldoen. In het bijzonder beoordelen zij welke processtappen moeten worden ondernomen om in voldoende mate de bescherming van persoonsgegevens met betrekking tot de gezondheid te waarborgen. De (team)manager is er verantwoordelijk voor dat binnen de FE aan de door de medisch adviseur opgestelde werkinstructies en adviezen wordt voldaan en de medewerkers in de FE het Reglement Functionele Eenheid naleven en ook op de hoogte worden gebracht

van nieuwe wet- en regelgeving of wijzigingen in bestaande wet- en regelgeving. Ook draagt hij zorg voor het ondertekenen van de geheimhoudingsverklaring. [VERTROUWELIJK] vindt een controle van dossiers plaats, waarbij ook de verwerking van persoonsgegevens waaronder persoonsgegevens betreffende de gezondheid aan de orde kan worden gesteld. Bij deze controles door de teamleiders zijn overigens de medisch adviseurs niet steeds betrokken.
Werkinstructies- en protocollen worden [VERTROUWELIJK] bekeken en aangescherpt. Ook toetst de FG en/of de [VERTROUWELIJK] periodiek of een en ander nog in lijn is met geldende wet- en regelgeving. In geval van wijzigingen worden de werkinstructies en -protocollen door de medisch adviseurs en teamleiders aangescherpt en binnen de FE's onder de aandacht gebracht.

Tijdens de interviews heeft Menzis aangegeven dat bij afwezigheid van een medisch adviseur de overige medisch adviseurs uit de andere FE('s) waarnemen. In dat geval wordt er rekening mee gehouden dat de waarnemend medisch adviseur geen adviseur is die werkt bij een FE die werkzaamheden verricht die niet mogen worden gecombineerd met de werkzaamheden van de te waarnemen FE (functiescheiding).

In het Reglement FE is opgenomen:
[VERTROUWELIJK]

Ook staat in het Reglement FE:
[VERTROUWELIJK]

Menzis heeft op verzoek van de AP de meest recente evaluatie van het functioneren van één van de functionele eenheden overlegd. [VERTROUWELIJK]

Menzis benadrukt dat de medisch adviseur niet de enige is die persoonsgegevens betreffende de gezondheid mag verwerken. Dit zou onwerkbaar zijn. De wet sluit niet uit dat declaraties met daarop DBC-codes door anderen dan medisch adviseurs (lees: een arts) worden verwerkt. De FE medewerkers die declaraties afhandelen staan echter wel onder leiding van de teammanager en van een medisch adviseur, zo heeft Menzis toegelicht. In concrete dossiers waarin de standaard werkprotocollen en -instructies onvoldoende houvast bieden, geven medisch adviseurs advies over de vraag of en welke persoonsgegevens betreffende de gezondheid noodzakelijk zijn en moeten worden opgevraagd. Een noodzakelijkheidsafweging wordt op dossierniveau gemaakt door de medisch adviseur indien een dossierbehandelaar daarom verzoekt. Het advies van de medisch adviseur wordt volgens de medisch adviseur in het dossier opgenomen, bijvoorbeeld door middel van vastlegging van een e-mail van die medisch adviseur.

Beoordeling

-geheimhouding

De AP stelt in de eerste plaats vast dat de medisch adviseurs die de FE's aansturen allen arts zijn en geregistreerd volgens de Wet BIG (BIG-geregistreerd). Daarmee rust op hen een geheimhoudingsplicht uit hoofde van beroep.[3] De AP stelt in de tweede plaats vast dat alle Menzis medewerkers beschikken over een geheimhoudingsplicht op grond van zowel een collectieve als een individuele arbeidsovereenkomst. FE-

[3] 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.

medewerkers tekenen daarnaast een extra geheimhoudingsverklaring. Voor telefoonmedewerkers geldt verder dat zij de eed of de belofte dienen af te leggen.

Gelet op het voorgaande komt de AP tot de conclusie dat door Menzis is voldaan 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 (medisch adviseurs) of een krachtens een overeenkomst (Menzis-medewerkers) onderworpen zijn aan een geheimhoudingsplicht.

-noodzakelijkheidsvereiste
Menzis heeft aan de rol van de medisch adviseur invulling gegeven door taken te beleggen in zogenaamde functionele eenheden waarin persoonsgegevens betreffende de gezondheid worden verwerkt onder verantwoordelijkheid van een medisch adviseur. De AP constateert dat de medisch adviseur een rol heeft bij het vóóraf opstellen en tussentijds aanpassen van werkinstructies, stappenplannen en waarborgen waar medewerkers zich aan moeten houden. Daarnaast zijn de medisch adviseurs beschikbaar voor adviezen aan FE-medewerkers en teamleiders over concrete situaties die afwijken van de standaard-werkinstructies. Bij afwezigheid van een medisch adviseur nemen de overige medisch adviseurs de FE('s) van de afwezige adviseur waar. De waarnemend medisch adviseur betreft een adviseur die niet werkt bij een FE die werkzaamheden verricht die vanwege functiescheidingsregels niet mogen worden gecombineerd met de werkzaamheden van de te waarnemen FE.

Gelet op het voorgaande komt de AP tot de conclusie dat Menzis met de door haar gekozen invulling van de rol van de medisch adviseur in beginsel afdoende 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.

Ten overvloede merkt de AP evenwel het volgende op. Het toezicht op de naleving van de door de medisch adviseur opgestelde werkinstructies is voor een groot deel belegd bij de teammanagers, die zelf geen medisch adviseurs zijn. [VERTROUWELIJK] Dat leidt op zichzelf niet tot een overtreding van de Wbp. De AP wijst er evenwel op dat in het door Menzis opgestelde regelement FE staat dat [VERTROUWELIJK]. Om de naleving van deze uitgangspunten te waarborgen, adviseert de AP Menzis om de betrokkenheid van de medisch adviseurs bij concrete gevallen, met name wanneer die afwijken van de werkinstructies, te intensiveren en vast te leggen in dossiers. Op deze manier wordt meer inzichtelijk op welke wijze een medisch adviseur in de dagelijkse praktijk betrokken is bij de verwerking van persoonsgegevens betreffende de gezondheid en de juiste uitwerking daarvan door medewerkers van Menzis.

-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 Menzis 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 Menzis op het punt van het medisch beroepsgeheim niet handelt in strijd met de Wbp.

Conclusies

Hieronder is per onderdeel een conclusie opgenomen.

Gedragscode en privacybeleid

Gelet op het gebruik van de Uniforme Maatregelen van ZN hanteert en de diverse eigen beleidsdocumenten, werkprocessen en werkinstructies van Menzis, is de AP van oordeel dat het enkele feit dat Menzis op haar website vermeldt dat zij toepassing geeft aan de gedragscode, die inmiddels is afgekeurd, niet reeds dat Menzis 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 Menzis die tot een nader onderzoek op dit punt dienen te leiden.

Doelbinding

De AP is niet gebleken van enige onrechtmatige verstrekkingen door Menzis aan derden nu sprake is van een wettelijke grondslag en in beginsel uitsluitend reguliere persoonsgegevens worden verstrekt en geen persoonsgegevens betreffende de gezondheid. Derhalve is niet gebleken dat Menzis voor dit doeleinde meer persoonsgegevens verstrekt dan noodzakelijk is en evenmin is gebleken dat Menzis persoonsgegevens verstrekt zonder dat daarvoor een wettelijke grondslag zou bestaan. De AP heeft bovendien geen aanwijzingen of signalen ontvangen die aanknopingspunten bieden voor een andere conclusie.

Ongeautoriseerde toegang tot persoonsgegevens

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.

Bewerkers

Uit de standaardovereenkomst en standaardtekst volgt dat Menzis toeziet op de correcte naleving van de Wbp. Bewerkers worden zo expliciet gewezen op de bijzondere eisen die gelden op grond van de Wbp ten aanzien van de verwerking van persoonsgegevens betreffende de gezondheid. De AP concludeert op grond hiervan dat door Menzis op dit punt 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 Menzis op het punt van het medisch beroepsgeheim niet handelt in strijd met de Wbp.
De AP concludeert namelijk dat persoonsgegevens betreffende de gezondheid binnen Menzis worden verwerkt door personen op wie een geheimhoudingsplicht rust uit hoofde van een beroep (medisch adviseurs) alsmede uit een overeenkomst (medewerkers Menzis). Gelet hierop komt de AP tot de conclusie dat Menzis 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 Menzis met de door haar gekozen invulling van de rol van de medisch adviseur in beginsel afdoende 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. Evenwel doet de AP Menzis op dit punt wel de aanbeveling om de betrokkenheid van de medisch adviseurs bij concrete gevallen, met name wanneer die afwijken van de werkinstructies, te intensiveren en vast te leggen in dossiers.
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 Menzis geen aanknopingspunten gevonden om aan de bevindingen van de NZa op dit punt te twijfelen.