

AAN AANGETEKEND
Ommelander Ziekenhuis Groep

DATUM 2 juni 2009

ONS KENMERK z2009-00215

CONTACTPERSOON

070 8888500

UW BRIEF VAN

UW KENMERK

ONDERWERP last onder dwangsom

Geachte A,

In het kader van hun toezichhoudende taak hebben de Inspectie voor de Gezondheidszorg (IGZ) en het College bescherming persoonsgegevens (CBP) in 2007 bij de Ommelander Ziekenhuis Groep, het St. Lucas Ziekenhuis (hierna: OZG of OZG Lucas voor zover het de locatie Lucas betreft) een onderzoek ingesteld naar de veilige toepassing van ICT en in het bijzonder de mate waarin de normen voor de informatiebeveiliging worden nageleefd. Naar aanleiding van dit onderzoek, het door het ziekenhuis vervolgens ingediende Plan van Aanpak, het voornemen van het CBP om gebruik te maken van zijn bevoegdheid om handhavend op te treden en uw schriftelijke zienswijze van 29 april 2009, kenmerk PvdW/hp 75, is tijdens het collegeoverleg van 2 juni 2009 besloten om een last onder dwangsom op te leggen.

De loop van de procedure

Op 1 juni 2007 hebben IGZ en CBP een bezoek gebracht aan het OZG Lucas in het kader van het hiervoor genoemde onderzoek.

Over de resultaten van dit onderzoek is een rapport met voorlopige bevindingen opgemaakt. Zoals in artikel 60 lid 2 Wet bescherming persoonsgegevens (Wbp) is bepaald, bent u in de gelegenheid gesteld uw zienswijze te geven op de voorlopige bevindingen van het onderzoek. U hebt van deze gelegenheid geen gebruik gemaakt. IGZ en CBP hebben vervolgens de definitieve bevindingen en conclusie vastgesteld.

Bij brief van 16 juli 2008 is u het rapport met de definitieve bevindingen en de conclusie naar aanleiding van het onderzoek toegezonden. IGZ en CBP concluderen dat er geen sprake is van een passend beveiligingsniveau zoals bedoeld in artikel 13 Wbp en dat evenmin is voldaan aan de voorwaarden om verantwoorde zorg te leveren zoals bedoeld in artikel 2 van de Kwaliteitswet zorginstellingen.

In de brief van 16 juli 2008 is u meegedeeld dat IGZ en CBP om die reden verwachten dat er vóór 15 oktober 2008 een Plan van Aanpak is opgesteld, waarin duidelijk wordt wat het ziekenhuis onderneemt om volledig aan de NEN 7510 norm te voldoen. In dit Plan van Aanpak dient expliciet uiteengezet te worden wat het ziekenhuis onderneemt om de in het rapport opgesomde

tekortkomingen op te lossen. Het zo nodig (opnieuw) uitvoeren van een risico-analyse dient deel uit te maken van het plan. In het plan moet in ieder geval worden aangegeven wanneer het ziekenhuis welk probleem zal hebben opgelost. Dat geldt voor alle onderwerpen die in de NEN 7510 aan de orde worden gesteld.

Ook is in de brief meegedeeld dat indien IGZ en CBP in het licht van de hiervoor genoemde eisen concluderen dat het ziekenhuis onvoldoende voortvarend werk maakt van het verbeteren van de informatiebeveiliging, IGZ en CBP zullen overwegen om handhavend op te treden.

Bij brief van 16 oktober 2008 heeft u IGZ uw Plan van Aanpak toegezonden, welk plan in kopie naar het CBP is gestuurd.

Bij brief van 26 maart 2009 heeft het CBP het ziekenhuis in kennis gesteld van zijn voornemen om handhavend op te treden.

Zienswijze

OZG heeft op 29 april 2009 bij het CBP een schriftelijke zienswijze ingediend.

Daarin staat dat er per 1 januari 2009 een fulltime informatiemanager is benoemd, die is aangemerkt als informatiebeveiligingsfunctionaris en dat in zijn takenpakket expliciet de implementatie van NEN 7510 in de OZG is opgenomen.

Het CBP heeft in de brief van de Raad van Bestuur d.d. 22 oktober 2008 en in het meegezonden functieprofiel niet aangetroffen dat de informatiemanager wordt aangemerkt als informatiebeveiligingsfunctionaris en evenmin wordt in zijn takenpakket de implementatie van de NEN 7510 genoemd.

Inzake het opstellen van een document voor de fysieke toegangsbeveiliging geeft het OZG aan dat het streven bestaat om in 2009 en 2010 te komen tot afgestemd toegangsbeveiligingsbeleid. Beide locaties van de OZG (locatie Delfzicht en locatie Lucas) hebben vanuit de historie hun toegangsbeveiliging op verschillende wijze georganiseerd.

Het CBP constateert dat een document, zoals dat omschreven is in de maatregel, niet aanwezig is in de meegestuurde documentatie. Een onderliggend basisdocument waarin wordt toegelicht waarom bepaalde maatregelen passend worden geacht bij een bepaald soort beveiligingszone, ontbreekt.

Voor wat betreft het opstellen en vaststellen van een document voor de toegangsbeveiliging van voorzieningen en gegevens, met als inhoud de regels en rechten voor elke gebruiker of groep van gebruikers, heeft de OGZ het CBP een aantal documenten gezonden. Het CBP heeft daarin de gevraagde maatregel niet aangetroffen.

Ten slotte stelt de OGZ dat de voormalige Melding Incidenten Patiëntenzorg wordt vervangen door een regeling voor Veilig Incidenten Melden (VIM). Men kiest daarbij voor een centrale (OGZ breed) en een decentrale (per afdeling) organisatie. Verder beschrijft de zienswijze dat de informatiemanager zal deelnemen in de centrale VIM.

De bij de zienswijze gevoegde stukken tonen niet de betrokkenheid van de informatiemanager bij de nieuwe incidentenmeldingenregeling aan en evenmin is deze opgenomen in het functieprofiel. Verder worden incidenten met de verwerking van persoonsgegevens of informatiebeveiligingsincidenten niet specifiek genoemd. Aan de maatregel is niet voldaan.

Handhavingsoverwegingen

Er is sprake van de verwerking van persoonsgegevens betreffende de gezondheid, op welke gegevens het medisch beroepsgeheim van toepassing is. De beveiliging van dergelijke persoonsgegevens moet voldoen aan de hoogste normen.

Uit het onderzoek ter plaatse is gebleken dat sprake is van overtreding van de normen. Het ziekenhuis is de mogelijkheid geboden via een Plan van Aanpak aan te tonen dat voortvarend wordt gewerkt aan maatregelen om de geconstateerde onrechtmatigheden op te heffen. Beide toezichthouders hebben geconcludeerd dat de door het ziekenhuis in het Plan van Aanpak hiertoe voorgenomen maatregelen onvoldoende zijn.

Hoewel de OZG in haar schriftelijke zienswijze heeft aangegeven dat zij denkt te voldoen aan de wettelijke bepaling van artikel 13 Wbp, blijkt dat aan de maatregelen in de brief van 26 maart 2009 niet is voldaan. De definitieve bevindingen van het onderzoek, het tijdsverloop in dit dossier en de ernst van de onrechtmatigheden geven het CBP voldoende aanleiding om verdere vervolgstappen te ondernemen ten opzichte van het ziekenhuis. Het CBP acht het opleggen van een dwangsom, teneinde te bewerkstelligen dat het ziekenhuis de overtredingen beëindigt, gerechtvaardigd.

Last onder dwangsom

Het CBP is ingevolge artikel 65 Wbp bevoegd bestuursdwang toe te passen ter handhaving van de bij of krachtens de Wbp gestelde verplichtingen. Op grond van artikel 5:32 eerste lid Algemene wet bestuursrecht (Awb) kan een bestuursorgaan dat bevoegd is bestuursdwang toe te passen in plaats daarvan de overtreder een last onder dwangsom opleggen.

Het CBP legt het ziekenhuis de volgende last onder dwangsom op. Het CBP sommeert het ziekenhuis om voor 1 september 2009 de volgende maatregelen te treffen:

- opstellen en vaststellen van een functieprofiel voor een informatiebeveiligingsfunctionaris (coördinator op het gebied van informatiebeveiliging);
- aanstellen of aanwijzen van een informatiebeveiligingsfunctionaris;
- opstellen en vaststellen van een document voor de fysieke toegangsbeveiliging, met een overzicht van welke beveiligingszones worden onderkend en per (type) beveiligde zone welke maatregelen moeten worden genomen;
- opstellen en vaststellen van een document voor de toegangsbeveiliging van voorzieningen en gegevens, met als inhoud de regels en rechten voor elke gebruiker of groep van gebruikers;
- het aanvullen van de bestaande regeling Melding Incidenten Patiëntenzorg met een onderdeel voor incidenten met de verwerking van persoonsgegevens.

Als toelichting op deze maatregelen wordt verwezen naar de NEN 7510, die als een gezaghebbende en sectorale uitwerking van artikel 13 Wbp wordt beschouwd.

Voor de datum van 1 september 2009 bent u geen dwangsommen verschuldigd. De aan u gegeven begunstigingstermijn is voldoende voor het doen beëindigen van de geconstateerde onrechtmatigheden..

Het CBP gelast u verder het CBP op de hoogte te brengen van het uitvoeren van deze maatregelen.

Indien u niet aan deze last voldoet, bent u vanaf 1 september 2009 per maatregel een dwangsom verschuldigd van €1000,- (duizend) per dag dat aan de maatregel niet is voldaan. Het bedrag waarboven geen dwangsom meer wordt verbeurd, wordt bepaald op €30.000,-. (dertigduizend) per maatregel.

De hoogte van de dwangsom is gerelateerd aan de ernst van de overtreding, aan de hoogte van de kosten die moeten worden gemaakt om de overtreding te beëindigen en aan het maatschappelijk belang van de naleving van de regelgeving.

Inwerkingtreding besluit

Op grond van de artikelen 3:40 en 3:41 van de Algemene wet bestuursrecht (Awb) treedt dit besluit onmiddellijk in werking.

Bezwaar

Ingevolge artikel 7:1 van de Algemene wet bestuursrecht kunt u tegen deze beschikking bezwaar maken door het indienen van een gemotiveerd bezwaarschrift, gericht aan het CBP, Postbus 93374, 2509 AJ Den Haag, onder vermelding van "Awb-bezwaar" op de enveloppe. De termijn waarbinnen het bezwaarschrift kan worden ingediend bedraagt zes weken na de dag waarop deze beschikking is verzonden.

Voorlopige voorziening

Indien u bezwaar heeft gemaakt, kunt u tevens gedurende de bezwaartermijn en ook daarna aan de rechter in uw arrondissement een verzoek doen om een voorlopige voorziening te treffen. Naar aanleiding daarvan kan de rechter de werking van het besluit schorsen. Voor het indienen van een verzoek om voorlopige voorziening bent u als indiener griffierechten verschuldigd. In dat geval ontvangt u een verzoek tot betaling van de rechtbank.

Het CBP verzoekt u, in het geval u een verzoek om een voorlopige voorziening zou indienen, daarvan een afschrift te doen toekomen aan het CBP.

Hoogachtend,

Het College bescherming persoonsgegevens,
Voor het College,

mr. J. Kohnstamm
voorzitter