

AAN AANGETEKEND
Rijnland Ziekenhuis

DATUM 2 juni 2009

ONS KENMERK z2009-00208

CONTACTPERSOON

070-8888500

UW BRIEF VAN

UW KENMERK

ONDERWERP last onder dwangsom

Geachte A,

In het kader van hun toezichthoudende taak hebben de Inspectie voor de Gezondheidszorg (IGZ) en het College bescherming persoonsgegevens (CBP) in 2007 bij het Rijnland Ziekenhuis 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 de hoorzitting van 29 april 2009, is tijdens het collegeoverleg van 2 juni 2009 besloten om een last onder dwangsom op te leggen.

De loop van de procedure

Op 7 juni 2007 hebben IGZ en CBP een bezoek gebracht aan het Rijnland Ziekenhuis 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. Bij brief van 23 april 2008 heeft u op deze bevindingen gereageerd. Met uw opmerkingen is rekening gehouden bij het vaststellen van het rapport definitieve bevindingen.

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

Bij brief van 2 april 2009 heeft het CBP het ziekenhuis in kennis gesteld van zijn voornemen om handhavend op te treden.

Zienswijze

Tijdens de hoorzitting op 29 april 2009 is het ziekenhuis in de gelegenheid gesteld om mondeling een zienswijze te geven ten aanzien van het voorgenomen besluit van 2 april 2009. Namens het ziekenhuis zijn op de hoorzitting verschenen: de heer R. Treffers (voorzitter van de Raad van Bestuur), de heer A.C. van der Berg (ICT-manager) en de heer J.A. van der Wel (adviseur). Van de hoorzitting is een verslag opgesteld. De heer Treffers heeft namens het ziekenhuis op het concept-verslag gereageerd, hetgeen er toe heeft geleid dat het verslag is aangepast. Het gewijzigde verslag is aan dit besluit gehecht.

De heer Van der Berg geeft aan dat de concept-risico-analyse gereed is en dat de rapportage daarover begin juni 2009 zal zijn afgerond of worden voorgelegd aan de Raad van Bestuur.

Hij deelt mee dat de functie van informatiebeveiligingsmanager is ondergebracht bij de secretaris van de Raad van Bestuur.

De heer Van der Berg deelt verder mee dat binnen de Raad van Bestuur mevrouw Molenaar is aangewezen als portefeuillehouder informatiebeveiliging.

Wat betreft de bewustwordingscampagne informatiebeveiliging geeft de heer Van der Berg aan dat de eerste fase hiervan is gestart in mei 2008 en dat deze campagne in mei 2009 wordt afgerond.

Ten slotte heeft het ziekenhuis ter zitting een map met aanvullende documentatie overhandigd aan het CBP.

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.

Risico-analyse informatiebeveiliging

In een vlak voor de hoorzitting gedateerd extern advies staat vermeld: "In de periode 2006-2009 zijn meerdere risicoanalyses gemaakt door externe organisaties waardoor de directie in deze periode een goed overzicht had en nog steeds heeft over de stand van zaken rond informatiebeveiliging." Vervolgens worden drie onderzoeken genoemd:

- onderzoek uit 2005. Dit onderzoek is verouderd;
- risico-analyse uit 2006. Dit onderzoek heeft zich geconcentreerd op continuïteitsrisico's. De overige beveiligingsrisico's zijn op dat moment niet nader onderzocht. Dit onderzoek is niet te beschouwen als een volwaardige en actuele risico-analyse;
- NEN 7510 scan (lopend). Deze scan wordt door het ziekenhuis ten onrechte als een risico-analyse gezien.

Hoewel het ziekenhuis tijdens de hoorzitting heeft aangegeven dat het denkt te voldoen aan de wettelijke bepaling van artikel 13 Wbp, blijkt uit de verkregen informatie dat zulks niet of nog niet het geval is. Aangezien er geen actuele risico-analyse is en deze evenmin in uitvoering is of wordt gepland, is aan de maatregel niet voldaan.

De definitieve bevindingen van het onderzoek, het tijdsverloop in dit dossier en de ernst van de onrechtmatigheden geven het CBP voldoende aanleiding om voor deze maatregel een dwangsom op te leggen, teneinde te bewerkstelligen dat het ziekenhuis de overtreding beëindigt.

Overige maatregelen

In het concept Plan van Aanpak Verbeteringen Informatieveiligheid van 28 april 2009 wordt bevestigd dat per juni 2009 een security officer zal worden aangesteld.

Tevens is ter zitting en uit de stukken gebleken dat een portefeuillehouder informatiebeveiliging binnen de Raad van Bestuur is aangewezen, mevrouw Molenaar.

Ten slotte is aangetoond dat de geplande bewustwordingscampagne informatiebeveiliging is uitgevoerd.

De eerder ter zake geconstateerde onrechtmatigheden blijken te zijn opgeheven, reden waarom het CBP met betrekking tot deze maatregelen afziet van verdere handhaving.

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:

- het uitvoeren van een risico-analyse informatiebeveiliging;
- het opstellen van een rapportage van de risico-analyse informatiebeveiliging.

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 de volgende dwangsom verschuldigd:

- een dwangsom van € 2000,- (tweeduizend) per dag dat de risico-analyse niet is uitgevoerd;
- een dwangsom van € 2000,- (tweeduizend) per dag dat de rapportage van de risico-analyse informatiebeveiliging niet is opgesteld.

Het bedrag waarboven geen dwangsom meer wordt verbeurd, wordt bepaald op €60.000,- (zestigduizend) 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 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 afschrift te doen toekomen aan het CBP.

Hoogachtend,

Het College bescherming persoonsgegevens,
Voor het College,

mr. J. Kohnstamm
voorzitter