



Inspectie Werk en Inkomen
*Ministerie van Sociale Zaken en
Werkgelegenheid*

Toetsing privacyregels bij arbodiensten

Nota van bevindingen

Nvb-Arbv 09/03, oktober 2009

Voorwoord

De burger mag verwachten dat het risico op misbruik en oneigenlijk gebruik van persoonsgegevens minimaal is. Uit de maatschappelijke discussie rond het Elektronisch Patiëntendossier blijkt dat de vastlegging van medische gegevens veel vragen op roept. Arbodiensten beschikken over persoonsgebonden medische gegevens. De minister van Sociale Zaken en Werkgelegenheid wijst instellingen aan die arbodiensten certificeren. Het is voor arbodiensten verplicht om zich te laten certificeren. De eisen waaraan een arbodienst moet voldoen, zijn vastgelegd in de Richtlijn Arbodiensten, waarin onder andere verwijzingen staan naar de Wet bescherming persoonsgegevens (Wbp).

Uit onderzoek van het College Bescherming Persoonsgegevens bleek dat de gecertificeerde arbodienst Tredin in strijd handelt met de Wbp. De Inspectie Werk en Inkomen heeft onderzocht hoe de certificerende instellingen (cki's) de naleving toetsen van de Wbp en andere privacybepalingen bij arbodiensten in het algemeen en bij Tredin in het bijzonder.

Dank zij de medewerking van de certificerende instellingen kon met een korte voorbereidingstijd het onderzoek in de maanden juni en juli worden uitgevoerd.

Drs. P.H.B. Pennekamp
Inspecteur-generaal a.i.

Inhoud

	Voorwoord	3
1	Inleiding	7
1.1	Kamervragen	7
1.2	Onderzoeksvragen	7
1.3	Onderzoeksmethode	7
2	Arbodiensten en cki's	9
2.1	Taken arbodiensten	9
2.2	Arbodiensten en cki's	9
2.3	De arbodienst en privacy	10
3	Handelwijze cki 1 bij Tredin B.V.	11
3.1	Inleiding	11
3.2	Handelwijze cki 1	11
3.3	Reactie cki op de casus Tredin B.V.	11
4	Handelwijze cki's bij de toetsing van privacy	13
4.1	De toetsing van privacy	13
4.2	Tekortkomingen en corrigerende maatregelen	14
5	Privacy als onderdeel van het ISO 9001 systeem	15
5.1	Algemene opzet audit	15
5.2	Tekortkomingen en corrigerende maatregelen	15
5.3	Privacy als onderdeel van ISO 9001	15
5.4	Toetsing door de Raad voor Accreditatie	16
6	Conclusies	17
6.1	Cki's zijn in staat om structurele privacyovertredingen te ontdekken	17
6.2	Cki's kunnen incidentele privacyovertredingen niet voorkomen	17
6.3	Naleving privacy is geen zwaarwegend beoordelingscriterium	17
6.4	Opvallend verschil handelwijze cki 1 met het CBP inzake Tredin B.V.	17
7	Reactie cki's	20
7.1	Toelichting	20
7.2	Reactie cki's	20
7.3	Nawoord IWI	20
	Lijst van afkortingen	22
	Bijlagen	23

1 Inleiding

1.1 Kamervragen

Eind maart 2009 heeft het College Bescherming Persoonsgegevens (CBP) een last onder dwangsom opgelegd aan de arbodienst Tredin B.V. wegens het herhaaldelijk overtreden van de privacyregelgeving. De dwangsom is 1000 euro per geconstateerde overtreding, met een maximum van 120.000 euro.

Een arbodienst heeft op grond van de Arbowet een certificaat nodig. Deze certificaten worden afgegeven door private instellingen, die daartoe door de minister van Sociale Zaken en Werkgelegenheid zijn aangewezen.

De Inspectie Werk en Inkomen houdt namens de minister van SZW toezicht op deze certificerende instellingen (cki's).

In april 2009 zijn Kamervragen gesteld waarin de minister is gevraagd een reactie te geven op de door het College Bescherming Persoonsgegevens op te leggen dwangsom aan de arbodienst Tredin B.V. wegens het doorspelen van medische dossiers aan de werkgevers. De minister heeft aan de vaste kamercommissie SZW aangegeven dat IWI een onderzoek zal uitvoeren.^{1,2}

1.2 Onderzoeksvragen

De minister heeft in mei 2009 IWI verzocht de handelwijze van cki 1 inzake Tredin B.V. te onderzoeken en tevens na te gaan of er zich soortgelijke casussen (kunnen) voordoen bij arbodiensten die door cki 1 of de andere cki's gecertificeerd zijn.³

Het onderzoek richt zich op overtredingen van arbodiensten bij de uitvoering van ziekteverzuimbegeleiding en die betrekking hebben op de privacybepalingen in het door de minister van SZW vastgestelde Reglement Certificatie Arbodiensten.

De onderzoeksvragen zijn:

1. Wat is de handelwijze van cki 1 (geweest) betreffende Tredin B.V.?
2. Hebben zich bij de andere certificerende instellingen met Tredin B.V. vergelijkbare casussen voorgedaan of kunnen deze zich voordoen?

1.3 Onderzoeksmethode

Het onderzoek is uitgevoerd bij alle cki's die tot 1 mei 2009 voor de certificering van arbodiensten waren aangewezen, namelijk: Bureau Veritas Certification Nederland B.V., Det Norske Veritas Certification B.V., Kiwa N.V. Certificatie en Keuringen en Lloyd's Register Nederland B.V.

Deze cki's worden in het rapport aangeduid met een willekeurig gekozen nummer.

De inspectie heeft interviews gehouden met auditors van de cki's die de arbodiensten toetsen en met functionarissen die op basis van die audits certificatiebeslissingen nemen. De interviewverslagen zijn door de cki's geaccordeerd. Met de interviews heeft de inspectie vastgesteld op welke wijze de cki's privacy toetsen als

¹ Brief vaste Kamercommissie SZW, kenmerk 2009Z06253/2009D19157.

² Brief van 27 april 2009, kenmerk: G&VW/AA/2009/9218.

³ Brief van 28 mei 2009, kenmerk G&VW/AA/2009/10225

onderdeel van het ISO 9001 systeem (zie hoofdstuk vijf). Daarnaast is de inspectie specifiek ingegaan op het toetsen van privacyregels in het kader van de ziekteverzuimbegeleiding door de arbodienst.

Waar mogelijk heeft de inspectie informatie uit de interviews getoetst aan de hand van gegevens uit de auditrapporten/dossiers van de cki's. In de auditrapporten heeft de inspectie weinig informatie gevonden over de wijze van toetsing van de naleving door de arbodienst van de privacyregels en de overwegingen die gehanteerd zijn om een geconstateerde tekortkoming te typeren (als licht of zwaar). De inspectie heeft daarom gebruik gemaakt van de meest recente controlebeoordelingen van de Raad voor Accreditatie waarin de uitvoering van de Richtlijn Arbodiensten door de cki's is getoetst.

2 Arbodiensten en cki's

2.1 Taken arbodiensten

De Arbeidsomstandighedenwet (Arbowet) verplicht werkgevers en werknemers tot zorg voor goede arbeidsomstandigheden. Voorts verplicht de Wet werk en inkomen naar arbeidsvermogen (WIA) de werkgever en de werknemer tot inspanningen om langdurig ziekteverzuim en beroep op deze wet zo veel mogelijk tegen te gaan. Deze wettelijke verplichtingen brengen voor de werkgever onder andere met zich mee dat hij zich voor de volgende taken deskundig laat bijstaan:

- advies en toetsing van de risicoinventarisatie en -evaluatie (RI&E);
- ziekteverzuimbegeleiding;
- arbeidsgezondheidskundig onderzoek;
- aanstellingskeuringen.

Doorgaans zal een werkgever gebruik maken van een interne of externe arbodienst waar deskundigen op het gebied van de genoemde vier taken werkzaam zijn.

2.2 Arbodiensten en cki's

Arbodiensten en cki's maken deel uit van het private stelsel van accreditatie en certificatie met een stichting met een Centraal College van Deskundigen (CCvD) dat verantwoordelijk is voor het beheer van de Regeling Certificatie Arbodiensten en met de Raad voor Accreditatie die controleert of de cki's hun werk goed doen.

De Regeling Certificatie Arbodiensten bestaat uit het Reglement Certificatie Arbodiensten en de Richtlijn Arbodiensten. De cki's hanteren naar de arbodienst toe de Richtlijn Arbodiensten en controleren jaarlijks of de arbodienst nog aan de certificatie-eisen voldoet. De richtlijn is een normatief document waarin alle eisen aan de kwaliteit van dienstverlening van een arbodienst staan. In deze richtlijn is aangegeven dat het certificaat van een arbodienst gebaseerd moet zijn op het ISO 9001 kwaliteitssysteem⁴, aangevuld met eisen/bepalingen uit wet- en regelgeving.

In juli 2008 is versie 7 van de Regeling Certificatie Arbodiensten vastgesteld door het CCvD. De verwijzing naar deze versie van de regeling is opgenomen in artikel 2.7 van de Arbeidsomstandighedenregeling, welke wijziging op 10 januari 2009 in werking is getreden (Staatscourant 200, nr. 350).

De cki's geven op basis van de regeling bij een positieve beoordeling per arbodienst een Certificaat Arbodienst af met een geldigheidsduur van drie jaar. Het certificaat geeft weer dat er een gerechtvaardigd vertrouwen bestaat dat de kwaliteit van dienstverlening overeenstemt met de Richtlijn Arbodiensten.⁵ Dat certificaat is zowel geldig voor het hoofdkantoor als voor alle vestigingen van een arbodienst.

⁴ Het kwaliteitssysteem omvat de organisatorische structuur, verantwoordelijkheden, bevoegdheden, procedures, processen en voorzieningen voor het ten uitvoer brengen van kwaliteitszorg (bron: zie vorige noot).

⁵ Regeling Certificatie Arbodiensten, 7^e versie d.d. juli 2008.

2.3 De arbodienst en privacy

Er gelden voor arbodiensten aanvullende eisen voor specifieke taken. De aanvullende eisen zijn waar mogelijk gekoppeld aan ISO 9001. De privacybepalingen zijn onderdeel van de aanvullende eisen.

Op het gebied van privacy zijn de volgende bepalingen in de Richtlijn Arbodiensten geformuleerd:

- Een arbodienst moet de regels naleven die zijn vastgelegd in de Wet bescherming persoonsgegevens (Wbp).
- Een arbodienst heeft een privacyreglement waarmee de toegang tot het persoonsgebonden medisch dossier beperkt blijft conform de KNMG-richtlijnen en waarmee de toegang tot andere zorg- of hulpverleningdossiers geregeld wordt.
- Een arbodienst beschikt over verklaringen beroepsgeheim of ondertekende geheimhoudingsverklaring van functionarissen die contact hebben met cliënten in het kader van individuele begeleiding.
- Een arbodienst beschikt over richtlijnen en adequate huisvesting en uitrusting waaruit blijkt dat de persoonlijke levenssfeer van de cliënten en de verzorgde werknemers wordt beschermd.

3 Handelwijze cki 1 bij Tredin B.V.

3.1 Inleiding⁶

In januari 2008 heeft het College Bescherming Persoonsgegevens (CBP) Tredin B.V. bezocht naar aanleiding van een klacht van een werknemer over het verstrekken van medische gegevens aan zijn werkgever door Tredin B.V. In een hoorzitting in januari 2009 geeft Tredin B.V. haar visie en maatregelen weer. Eind maart 2009 legt het CBP een last onder dwangsom op aan Tredin B.V. Het CBP voert als reden aan: "Hoewel de arbodienst reeds op 3 juni 2008 op de hoogte is gesteld van de voorlopige bevindingen van het onderzoek, heeft het CBP tijdens de hoorzitting van 21 januari 2009 moeten vaststellen dat de door de arbodienst getroffen maatregelen onvoldoende zijn om de geconstateerde onrechtmatigheden op te heffen."

3.2 Handelwijze cki 1

Cki 1 is via de media op de hoogte gekomen van de zaak Tredin B.V. en de rapportage van het CBP. Er is geen contact geweest met het CBP voor en na de publicatie. De inspectie heeft de auditrapporten van cki 1 over Tredin B.V. opgevraagd. De verslaglegging in de auditrapporten is tot hoofdlijnen beperkt. In de auditrapporten ontbreken de overwegingen die cki 1 heeft gehanteerd, en de weging daarvan, bij het bepalen van de corrigerende maatregelen inzake Tredin B.V.

Cki 1 heeft de door het CBP geconstateerde overtredingen bij naleving van regelgeving in zijn audit in februari 2009 met Tredin B.V. besproken. Cki 1 heeft in de handelwijze van de arbodienst geen reden gezien om dit als een kritieke, major nonconformity⁷ aan te merken. Cki 1 concludeert: "De arbodienst voldoet nog steeds aan de eisen van de richtlijn arbodiensten".

In juni 2009 voert cki 1 een ingelaste audit bij Tredin B.V. uit naar de door Tredin B.V. uitgevoerde oorzaakanalyse en de te nemen/genomen beheersmaatregelen. Tredin B.V. geeft aan ook de houding en gedrag medewerkers inzake het zorgvuldig omgaan met privacygevoelige informatie aan te pakken.⁸ Ter borging van de genomen maatregelen zal Tredin B.V. privacy als vast onderdeel van de interne audit aan bod laten komen. In het auditrapport van cki 1 ontbreekt de weging van de situatie bij Tredin B.V. Uit het feit dat pas bij het surveillancebezoek in februari 2010 extra aandacht zal worden besteed aan de interne (Tredin)audits op het privacyaspect is wel te concluderen dat het voor cki 1 niet gaat om een major nonconformity.

3.3 Reactie cki op de casus Tredin B.V.

Tredin B.V. is volgens cki 1 geen incident. Wel kan het zijn dat de werkwijze van deze arbodienst de kans op overtredingen heeft vergroot. Bij verzuimtrajecten komen bij Tredin B.V. bedrijfsartsen vaak pas na de arbeidsdeskundige in beeld. Het is mogelijk dat de privacyaltherheid bij andere medewerkers niet zo hoog is als bij artsen. Dit wordt een aandachtspunt bij de audits van cki 1. Cki 1 geeft aan kriti-

⁶ Bron voor deze paragraaf: College Bescherming Persoonsgegevens, brief met kenmerk Z2008-01482.

⁷ Bij een major nonconformity moet de tekortkoming binnen drie maanden opgelost zijn.

⁸ Bron: Rapport cki 1 van 8 juli 2009 over de audit van Tredin op 30 juni 2009

scher te willen kijken naar privacyaspecten maar geen fundamenteel andere manier van auditen te gaan toepassen.

4 Handelwijze cki's bij de toetsing van privacy

4.1 De toetsing van privacy

De cki's geven aan dat bescherming van persoonsgegevens (privacy) maar één van de aspecten is die in een audit aan de orde kan komen. Het is geen specifiek en regulier thema voor toetsing en rapportage. Er wordt door de auditors niet met een vooropgezet plan naar mogelijke overtredingen gezocht, maar deze kunnen bij de uitvoering van een audit wel naar voren komen. Privacyaspecten worden procesmatig getoetst (zijn er voldoende beheersmaatregelen). De cki's geven in de interviews aan dat bij voldoende aanleiding meer op detailniveau naar het proces gekeken wordt. In onderstaande tekstblokken wordt geïllustreerd hoe de toetsing op de privacy tijdens een audit in zijn werk gaat. Hieruit blijkt dat de cki's de privacybepalingen in de Richtlijn Arbodiensten op een verschillende manier toetsen. Er is wat betreft de toetsing van privacy dus geen sprake van uniformiteit in de uitgevoerde audits.

c k i 7	Auditors toetsen naleving van privacyaspecten o.a. door na te gaan hoe de toegang tot (elektronische) medische dossiers beveiligd is, hoe specifieke functionarissen omgaan met het reglement en door het feitelijke proces bij een aantal verzuimtrajecten te vergelijken met vooraf vastgelegde stappen en procedures. Er wordt bij de audit alleen als er een aanleiding voor is, gericht gekeken in de persoonsdossiers en brieven met als oogmerk om deze inhoudelijk te beoordelen op overtredingen. E-mail verkeer wordt niet als een apart thema beoordeeld bij audits. Het zou in theorie wel kunnen, maar dan als onderdeel van het beoordelen van een bepaald bedrijfsproces waarbij e-mailverkeer een onderdeel is.
c k i 2	De audit op privacyaspecten bestaat uit een beoordeling van het administratieve proces en een gesprek met de bedrijfsarts van de arbodienst. Er wordt onder andere gekeken naar: de wijze waarop de arbodienst communicatie over privacyaspecten heeft geregeld, hoe de geheimhouding is geregeld en welke toegangsborging het ICT-systeem bevat ten aanzien van het medische deel. De auditor gaat ook het systeem in om dieper door te kijken, waarbij ook patiëntendossiers aan bod komen (ongeveer 5). Hiervoor vraagt men uitdrukkelijk toestemming van de arbodienst.
C k i 3	Bij de interviews bij de bedrijfsarts van de arbodienst wordt aan de hand van een case het traject van verzuimbegeleiding nagelopen. Er vindt geen rapportage op detailniveau plaats, dit heeft alles te maken met de geheimhoudingsverklaring van de auditors. De auditors daarbij gaan zo diep het systeem in als ze nodig achten. Er wordt zonodig ingelogd in het systeem en gekeken in brieven en e-mails. Dit is een onderdeel van de systeemcheck en niet bedoeld als opsporingsmethode. De bij de audit betrokken bedrijfsarts voert dit deel van de toets veelal uit. Andere disciplines zoals veiligheidskundige en arbeidshygiënist toetsen dit onderdeel ook.
c k i 4	Bij de audits komt het bij de implementatietoets voor dat wordt ingelogd op het systeem en brieven en/of e-mails zijn bekeken. Randvoorwaarde is dat ook cki's aan privacyregels zijn gebonden. De bedrijfsarts in het auditteam neemt dit voor zijn rekening. Het gaat om systeemtoetsing aan de hand van de Richtlijn Arbodiensten, die certificering mogelijk moet maken. Het gaat niet om het gericht zoeken naar afwijkingen.

4.2 Tekortkomingen en corrigerende maatregelen

In de interviews geven cki 1 en cki 2 aan dat privacy gelijkwaardig is aan de andere toetspunten en dat tekortkomingen niet anders wordt gewogen. Voor cki 3 wegen privacyaspecten wat zwaarder omdat "specifiek aan de Richtlijn Arbodiensten wordt getoetst". Cki 4 geeft aan dat het niet naleven van (privacy)wetgeving al snel beoordeeld zal worden als een grote tekortkoming.

Cki 2 heeft aangegeven weinig overtredingen op het gebied van privacyregels waar te nemen. Wel heeft cki 2 wel eens opmerkingen in audits gemaakt. Het ging bijvoorbeeld om brieven van bedrijfsartsen aan de werkgevers waarin zaken staan die mogelijk in het grensgebied liggen van wat toelaatbaar is. Ook is volgens cki 2 de toegangsborging tot het medische deel in de ICT een aandachtspunt. Dat heeft vaak te maken met de toedeling van werkzaamheden aan medewerkers die feitelijk niet met de verwerking van medische gegevens belast moeten zijn.

Door cki 3 en cki 4 zijn geen overtredingen op het gebied van privacy bij de door hen gecertificeerde arbodiensten geconstateerd. In de door de inspectie onderzochte dossiers bij cki 2, cki 3 en cki 4 is geen informatie aangetroffen over de wijze van toetsing van privacyregels en eventuele tekortkomingen op dit gebied.

Cki 1 heeft wel overtredingen geconstateerd. Uit de auditrapporten bleek het te gaan om overtredingen als:

- Het privacyreglement maakt geen melding van het bestaan van een medisch dossier en de toegangsrechten daartoe.
- De arbodeskundige rapportages zijn in het computersysteem vrij toegankelijk. Er is geen werkend autorisatiesysteem.
- Bij de terugkoppeling van de spoedcontrole krijgt de werkgever medische gegevens over de werknemer.

Deze overtredingen zijn alle als een kleine tekortkoming (minor nonconformity) getypeerd.

5 Privacy als onderdeel van het ISO 9001 systeem

5.1 Algemene opzet audit

De cki's geven in de interviews aan bij de toetsing van de certificatie-eisen gekozen te hebben voor een opzet waarbij deskundigen de audits uitvoeren en de verslaglegging tot hoofdlijnen beperkt blijft. In het Reglement Certificatie Arbodiensten staan de deskundigheidscriteria waaraan de auditors van de cki moeten voldoen (in termen van opleiding, ervaring en bekwaamheid). De cki's geven aan dat de auditors goed toegerust zijn om privacyovertredingen vast te kunnen stellen. In het reglement is eveneens aangegeven hoeveel auditdagen een cki maximaal mag besteden aan de certificatie van arbodiensten. Het maximale aantal auditdagen is afhankelijk van het aantal personeelsleden en het aantal vestigingen van een arbodienst. De voorgeschreven maximale auditdagen zijn volgens de cki's voldoende voor de systeemtoets op privacyaspecten, maar niet voor een verdieping.

De audit is gericht op de toetsing van het primaire proces van de arbodienst aan de ISO 9001-norm. In de praktijk betekent dit: "De essentiële indicatoren van effectief functioneren van het managementsysteem worden elk regulier bezoek beoordeeld. Dit gebeurt tijdens een gesprek met het top management en bij de beoordeling van de geselecteerde processen en thema's. Tot deze indicatoren behoren interne audits en directiebeoordelingen; de acties die zijn ondernomen op de nonconformities uit eerdere audits; de behandeling van klachten, [...] de voortgang bij de uitvoering van verbeteracties; de beheersing van operationele processen; wijzigingen in het management systeem [...]. De definitieve bepaling van auditthema's gebeurt na de beoordeling van de actuele prestaties en wijzigingen."⁹

5.2 Tekortkomingen en corrigerende maatregelen

Auditors van de cki kunnen vaststellen dat het primaire proces van de arbodienst (deels) niet voldoet aan de certificatie-eis en/of de benodigde output niet levert. De cki's hanteren hierbij verschillende gradaties. Bij de lichtste gradatie is er sprake van een opmerking over een situatie die mogelijk kan leiden tot een tekortkoming. Een tekortkoming is een belemmering voor het toekennen of het behoud van het certificaat. Bij een kleine tekortkoming (minor nonconformity) moet de arbodienst aangeven hoe ze de afwijking zal verhelpen en vindt de verificatie plaats bij de volgende periodieke audit (veelal een jaar later). Bij een grote, 'kritische' tekortkoming (major nonconformity) moet de arbodienst de tekortkoming op korte termijn (veelal binnen drie maanden) oplossen en zal de cki de implementatie van het herstel van de tekortkoming vervolgens in een ingelaste audit toetsen.

5.3 Privacy als onderdeel van ISO 9001

De belangrijkste eis voor een arbodienst om een certificaat te verkrijgen, is het beschikken over een ISO 9001 kwaliteitssysteem. De Richtlijn Arbodiensten bevat een specifieke uitwerking of interpretatie van het ISO 9001 kwaliteitssysteem waar de arbodienst over dient te beschikken. De privacyregels in de Richtlijn Arbodiensten vallen onder het hoofdstuk 'Management van middelen' uit ISO 9001. Vanuit het

⁹ Toelichting die een cki geeft in alle auditrapporten, de andere cki's hanteren een soortgelijke opzet.

perspectief ISO 9001 dienen organisatie aan te tonen dat ze in staat zijn (qua inrichting en opzet) om producten te leveren die voldoen aan de eisen van de klant en de regels na te leven die in de Wet bescherming persoonsgegevens zijn opgenomen. Cki's gebruiken interviews met deskundigen en reacties van de klanten (klanttevredenheid en klachten) als indicatoren voor mogelijke tekortkomingen op systeemniveau die kunnen leiden tot diepgaander onderzoek. Een ISO 9001 auditor is volgens de cki's geen handhaver of opsporingsambtenaar en zal niet gericht de naleving van privacyregels in de praktijk toetsen.

5.4 Toetsing door de Raad voor Accreditatie

De vier cki's zijn geaccrediteerd door de Raad voor Accreditatie (RvA) op basis van de norm ISO/IEC 17021. Deze norm is van toepassing op certificatie-instellingen die managementsystemen (op grond van ISO 9001) certificeren. De drie cki's die momenteel arbodiensten certificeren, hebben de Richtlijn Arbodiensten (zie paragraaf 2.2) als een specifiek normatief document laten onderbrengen in de ISO/IEC 17021 accreditatie.¹⁰ De 17021 kent geen minor nonconformiteiten. Dit type afwijking zal daarom weinig aandacht van de RvA beoordelaars krijgen. De RvA kan bij de cki's de privacyelementen nadrukkelijker gaan controleren, maar dit moet dan via aanpassing van de Richtlijn Arbodiensten geregeld worden.

De inspectie heeft de meest recente controlebeoordelingen van de RvA doorgenomen waarin de uitvoering door de cki's van de Richtlijn Arbodiensten is getoetst. Bij cki 1 en cki 3 is de controlebeoordeling recent (2008) uitgevoerd. Bij cki 2 en cki 4 heeft de RvA in 2007 respectievelijk 2006 de uitvoering door cki's op delen van de regeling beoordeeld. De RvA kan haar controlebeoordeling onder andere laten bestaan uit een bijwoning¹¹.

In het beoordelingsrapport van cki 3 worden de resultaten van de bijwoning vermeld. De RvA constateert dat de cki tijdens het interview met (de vervanger voor) de bedrijfsarts verzuimbegeleiding, PAGO, arbeidsomstandighedenspreekuur en aanstellingskeuringen aan de hand van de procedures heeft geverifieerd. De RvA merkt op dat alleen de procedures zijn geverifieerd en er geen aandacht is geweest voor de inhoudelijke kant van deze kerntaken. De RvA concludeert dat het eindgesprek van de cki met de arbodienst voldoet aan de gestelde eisen.

In de controlebeoordelingen bij cki 1, cki 2 en cki 4 heeft de RvA geen grote tekortkomingen geconstateerd ten aanzien van de wijze waarop de cki's de Richtlijn Arbodiensten uitvoeren. Deze cki's hebben een geldige ISO/IEC 17021 accreditatie.

De inspectie concludeert hieruit dat de cki's handelen in overeenstemming met de procedurele eisen voor de controle en certificering van arbodiensten.

¹⁰ Bij één cki is per 1 mei 2009 de aanwijzing op eigen verzoek ingetrokken.

¹¹ Het in de praktijk waarnemen van activiteiten die door de instelling worden uitgevoerd, zoals testen, kalibraties, inspecties, audits en examens.

6 Conclusies

6.1 Cki's zijn in staat om structurele privacyovertredingen te ontdekken

De handelwijze van de cki's voldoet aan de accreditatienorm ISO/IEC 17021. Dit wil zeggen dat de cki's de arbodiensten op systeemniveau conform de eisen controleren en certificeren. De cki's kunnen op deze wijze structurele overtredingen van de privacywet constateren. De cki's geven in de interviews aan over voldoende mogelijkheden te beschikken om overtredingen vast te stellen.

6.2 Cki's kunnen incidentele privacyovertredingen niet voorkomen

De werkwijze volgens ISO 9001 is gericht op het managementsysteem en zijn processen. Met de huidige werkwijze van de cki's worden incidentele overtredingen van privacyregels alleen bij toeval ontdekt. Te verwachten valt dat er uit het lopende CBP-onderzoek bij andere arbodiensten ook overtredingen geconstateerd zullen worden. De cki's onderkennen dit zelf. Cki 1 stelt dat overtredingen als bij Tredin B.V. bij ISO 9001 systeemcertificatie eigenlijk, vanwege het steekproefsgewijze onderzoek, niet altijd geconstateerd kunnen worden: "Als partijen of mensen willens en wetens de regels willen overtreden, kan dit altijd wel en hoeft dit niet altijd bij een systeemaudit boven tafel te komen".

6.3 Naleving privacy is geen zwaarwegend beoordelingscriterium

In de Richtlijn Arbodiensten staan geen uitgewerkte voorschriften voor de controle op en weging van privacy. De cki's hebben de richtlijn zelf niet nader uitgewerkt. De cki's hebben dus een grote discretionaire bevoegdheid.

Cki 1 en cki 2, de twee cki's met een groot marktaandeel, geven aan privacy niet anders te wegen dan andere toetspunten uit het Reglement Certificatie Arbodiensten. In het onderzoek heeft de inspectie alleen bij cki 1 privacyovertredingen in de dossiers aangetroffen. Deze zijn alle als een kleine tekortkoming getypeerd. De inspectie vindt het opvallend dat de cki's de naleving van privacyregels geen zwaarwegend beoordelingscriterium vinden voor het functioneren van een arbodienst. De casus Tredin heeft daarin geen verandering gebracht. Van instellingen die aangewezen worden door de minister van SZW mag verwacht worden dat ze oog hebben voor het (publieke) belang van privacy. De cki's laten zich nu bij de weging van nonconformiteiten (major of minor) vooral sturen door het schema. Indien het maatschappelijk relevant is dat tekortkomingen in de privacysfeer als "major" worden aangemerkt, dan zal de schemabeheerder (SBCA) dat nadrukkelijk in zijn schema moeten vastleggen.

6.4 Opvallend verschil handelwijze cki 1 met het CBP inzake Tredin B.V.

Cki 1 heeft de overtredingen bij de arbodienst Tredin B.V. zelf niet ontdekt. Wel zijn de bevindingen van het CBP in de audit van cki 1 van februari 2009 aan bod gekomen. Cki 1 heeft geen reden gezien om de arbodienst te verplichten om op korte termijn de tekortkoming op te lossen. Voor het CBP waren de maatregelen van de

arbodienst onvoldoende en de reden om een last onder dwangsom op te leggen. Cki 1 constateert in een ingelaste audit in juni 2009 dat Tredin B.V. maatregelen heeft getroffen en geeft aan om in een volgende audit (februari 2010) de implementatie daarvan te beoordelen. Het is opvallend dat cki 1 bij een maatschappelijk gevoelige casus als Tredin B.V. deze casus niet als een major nonconformity behandelt. Dat is een opvallend verschil met de weging van het CBP betreffende Tredin B.V.

7 Reactie cki's

7.1 Toelichting

De Inspectie Werk en Inkomen heeft de conceptrapportage voor een bestuurlijke reactie voorgelegd aan de cki's die tot 1 mei 2009 voor de certificering van arbodiensten waren aangewezen. Dit zijn Bureau Veritas Certification Nederland B.V., Det Norske Veritas Certification B.V., Kiwa N.V. Certificatie en Keuringen en Lloyd's Register Nederland B.V.

Deze cki's worden in het rapport aangeduid met een willekeurig gekozen nummer.

In dit hoofdstuk is de kern van de reacties weergegeven. De volledige reacties van de cki's zijn als bijlage toegevoegd.

7.2 Reactie cki's

Bureau Veritas Certification Nederland B.V. heeft geen bestuurlijke reactie gegeven. Det Norske Veritas Certification B.V. heeft geen bezwaar tegen de inhoud van het rapport.

Kiwa N.V. Certificatie en Keuringen onderschrijft de conclusies van de inspectie en geeft aan het niet voldoen aan privacyregels als een zwaarwegend punt in de beoordeling te beschouwen.

Lloyd's Register Nederland B.V. geeft een uitgebreide toelichting bij de paragrafen 1.3, 3.2 en 4.1 van het rapport. Lloyd's wijst in zijn reactie op normen die beschikbaar zijn voor medische informatiebeveiliging en geeft aan desgevraagd nadere informatie over de toepasbaarheid van deze normen beschikbaar te willen stellen.

7.3 Nawoord IWI

De reacties van de cki's hebben geen aanleiding gegeven om de conclusies van de inspectie aan te passen. Wel zijn enkele tekstuele wijzigingen doorgevoerd.

Lijst van afkortingen

CBP	College Bescherming Persoonsgegevens
CcvD	Centraal College van Deskundigen
Cki	Certificatie- en keuringsinstelling
ICT	informatie- en communicatietechnologie
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IWI	Inspectie Werk en Inkomen
PAGO	Periodiek arbeidsgezondheidskundig onderzoek
RvA	Raad voor Accreditatie
SBCA	Stichting Beheer Certificatie Arbodiensten
SZW	(Ministerie van) Sociale Zaken en Werkgelegenheid
Wbp	Wet bescherming persoonsgegevens

Bijlagen

Reactie Det Norske Veritas Certification B.V.

Reactie Kiwa N.V. Certificatie en Keuringen

Reactie Lloyd's Register Nederland B.V.

DET NORSKE VERITAS



Inspectie Werk en Inkomen
Ministerie van Sociale Zaken en Werkgelegenheid
drs. P.H.B. Pennekamp
Wilhelmina van Pruisenweg 52
Postbus 11563
2502 AN Den Haag

DET NORSKE VERITAS
CERTIFICATION BV
DNV Industry
Region North and West Europe
Zwolseweg 1
Barendrecht - 2994 LB
Netherlands
Tel: +31 (0) 102922688
Fax: +31 (0) 104796768
http://www.dnv.com
KvK nr. 24273935

Barendrecht, 25 september 2009

Onderwerp: Bestuurlijke reactie IWI conceptrapport certificatie arbodiensten

Geachte heer Pennekamp,

Wij hebben het rapport doorgenomen en geen bezwaar tegen de informatie zoals die in het rapport is opgenomen.

Ten aanzien van uw verzoek om de naam van DNV in het rapport te noemen ipv [REDACTED] moet ik afwijzend reageren.

Ik hoop u hiermee van voldoende te hebben geantwoord.

Anders Lindgren
Country Manager
DNV Certification B.V

Nr: IWI / 2009 / 3391	
ter behandeling	afschrift
ARW	
ontv.	29 SEP 2009
dossier	2129.000/3

Nr: IWI / 2009/3394	
ter behandeling	afschrift
ARBU	
ontv. 29 SEP 2009	
dossier	
2129.000/3	

Inspectie Werk en Inkomen
T.a.v. de heer drs. P.H.B. Pennekamp
Postbus 11563
2502 AN 'S-GRAVENHAGE

Kiwa N.V.
Sir W. Churchill-laan 273
Postbus 70
2280 AB RIJSWIJK

Tel. 070 414 44 00
Fax 070 414 44 20
E-mail info@kiwa.nl
www.kiwa.nl

Onderwerp IWI-onderzoek certificering arbodiensten
Informatie Richard Meijburg, 4537
E-mail Richard.Meijburg@kiwa.nl
Datum 28 september 2009
Kenmerk 0909280952RM

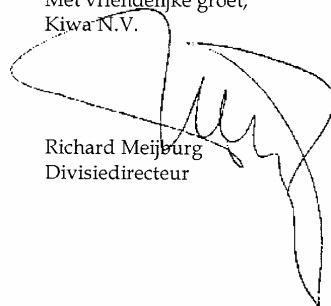
Geachte heer Pennekamp,

In reactie op uw brief van 18 september 2009, waarin u ons uitnodigt om te reageren op de conclusies in het IWI-onderzoek Toetsing privacyregels bij arbodiensten, het volgende.

- 6.1 Wij onderschrijven de conclusie dat wij over voldoende mogelijkheden beschikken om structurele overtredingen van de privacywet te constateren.
- 6.2 Wij onderschrijven de conclusie dat incidentele overtredingen van de privacyregels alleen bij toeval ontdekt worden. Wij willen daaraan toevoegen dat structurele overtredingen alleen langere tijd onopgemerkt blijven indien men willens en wetens de regels wil overtreden, maar dan is er in feite sprake van opzettelijke misleiding. Certificatie is gebaseerd op vertrouwen en richt zich op een professionele organisatie.
- 6.3 Wij zijn van mening dat het niet voldoen aan de privacyregels een zwaarwegend punt in de beoordeling is. Het niet voldoen aan de privacyregels zal daarom door ons als een kritische tekortkoming worden gekwalificeerd. Tot op heden hebben wij een dergelijke tekortkoming niet geconstateerd, terwijl wij op het punt van privacyregels wel getoetst hebben (dit in tegenstelling tot hetgeen in artikel 4.2 van het rapport wordt gesteld).
- 6.4 Een kritische tekortkoming moet binnen een vastgestelde periode worden gecorrigeerd en ter voorkoming van herhaling moet een corrigerende maatregel worden getroffen waarvan de implementatie door ons wordt geverifieerd binnen de gestelde periode.

Met vriendelijke groet,
Kiwa N.V.

Richard Meijburg
Divisiedirecteur



Handelsregister Regio
Haaglanden, 27039108



www.lrq.nl

Customer Services: +31 (0)10 201 84 01
Training Services: +31 (0)10 201 84 45
Sales & Contacts: +31 (0)10 201 84 76
Fax: +31 (0)10 201 84 95
E-mail: info@lrqa.nl

LRQA – Lloyd's Register Nederland B.V.

P.O. Box 701
3000 AS Rotterdam
Weena Zuid 170
3012 NC Rotterdam
The Netherlands

Inspectie Werk en Inkomen
Ministerie van Sociale Zaken en Werkgelegenheid
De heer drs. P.H.B. Pennekamp
Postbus 11563
2502 AN Den Haag

Nr: IW1/ 2009/3393	
ter behandeling	afschijn
ARBU	
oniv.	29 SEP 2009
dossier	2129.000/3

24 september 2009

Kenmerk: JPR-148

Betref: reactie op concept rapportage "Toetsing privacyregels bij arbodiensten", d.d. 15 september 2009.

Geachte heer Pennekamp,

Ingevolge uw verzoek, brief kenmerk 2009/3308, d.d. september 2009, kan ik u het volgende meedelen.

Reactie op het betreffende rapport is per hoofdstuk en/of paragraaf hierna vermeld.

1.3

De informatie in auditrapporten is in het algemeen gebaseerd op bevindingen in verband met genomen steekproeven. Eventueel geconstateerde afwijkingen worden gerapporteerd. Indien geen specifieke informatie over een aspect is beschreven, wil dit overigens niet zeggen dat het onderwerp niet aan de orde is geweest.

3.2

Tijdens het reguliere jaarlijkse bezoek is door één van de auditoren vastgesteld dat naar aanleiding van een onderzoek van het CBP m.b.t. overtreding van privacy regels t.a.v. medische persoonsgegevens, een werkgroep is gestart om e.e.a. op te volgen. Aangezien deze actie inmiddels in gang was gezet, heeft de auditor dit als een aandachtspunt voor het volgende auditbezoek in de constateringentabel van het auditrapport opgenomen (0902EDQ04).

A member of the Lloyd's Register Group.

A company registered at the Chamber of Commerce in Rotterdam under number 24247948. Our general terms and conditions LRQA shall apply to any agreement.
A network of offices worldwide.



www.lrqa.nl
 Customer Services: +31 (0)10 201 84 01
 Training Services: +31 (0)10 201 84 45
 Sales & Contracts: +31 (0)10 201 84 76
 Fax: +31 (0)10 201 84 95
 E-mail: info@lrqa.nl

LRQA – Lloyd's Register Nederland B.V.
 P.O. Box 701
 3000 AS Rotterdam
 Weena-Zuid 170
 3012 NC Rotterdam
 The Netherlands

Mede naar aanleiding van de berichtgeving in de media, alsmede de rapportage van het CBP is door de lead auditor met Tredin een afspraak gemaakt voor een extra tussentijds bezoek (special surveillance) i.v.m. de beoordeling van de oorzaakanalyse, de te nemen en/of genomen maatregelen, alsmede de borging. Op grond van zijn beoordeling van deze oorzaakanalyse en plan van aanpak is de auditor van mening dat een nieuw tussentijds bezoek aan Tredin niet noodzakelijk was en is aangegeven dat dit onderwerp bij het eerstkomende bezoek extra aandacht zal krijgen. Om deze reden is niet alsnog een Major Non Conformity uitgeschreven.

4.1

Certificatie van arbodiensten betreft systeemtoetsing en geen inspectie. Medische dossiers kunnen worden ingezien in het kader van de toetsingen van de diverse processen (bijvoorbeeld verzuimbegeleiding en reïntegratie). Afhankelijk van de constatering kan de steekproef worden uitgebreid om een goed en evenwichtig beeld te krijgen van de beheersing van de diverse processen.

Het huidige certificatiesysteem (Regeling Certificatie Arbodiensten) wordt beheerd door het Centraal College van Deskundigen –SBCA, waarin onder andere zitting hebben vertegenwoordigers van werkgevers en werknemers, arbodiensten (Boaborea), certificatie-instellingen alsmede waarnemers/toehoorders van SZW en TNC Kwaliteit van leven als adviseur. Daarnaast worden jaarlijks zg. harmonisatiedagen georganiseerd waarin onder andere audit-ervaringen en ontwikkelingen aan de orde komen en waarin bovengenoemde partijen eveneens participeren.

Overigens kan nog worden opgemerkt dat in de concept versie van het "certificatieschema voor de dienstverlening door arbodiensten", d.d. april 2009, (pag. 30/43) min of meer dezelfde bepalingen m.b.t. privacy zijn opgenomen als in de huidige 7^e versie. Wel is in de concept versie (pag. 14/43) aangegeven dat het schenden van privacy voorschriften door een arbodienst als rechtspersoon en/of medewerkers van een arbodienst een ernstig feit is, met grote gevolgen voor de betrokken werknemer.

Algemeen

Binnen de Zorg is momenteel veel aandacht voor medische informatiebeveiliging. Hiervoor zijn twee specifieke normen beschikbaar, te weten NEN 7510 "Medische informatica-Informatiebeveiliging in de zorg-Algemeen" en NEN 7511-1 "Medische informatica- Informatiebeveiliging in de zorg-Toetsbaar voorschrift bij NEN 7510 voor complexe organisaties".



www.lrqa.nl		LRQA – Lloyd's Register Nederland B.V.
Customer Services:	+31 (0)10 201 84 01	P.O. Box 701
Training Services:	+31 (0)10 201 84 45	3000 AS Rotterdam
Sales & Contracts:	+31 (0)10 201 84 76	Weena-Zuid 170
Fax:	+31 (0)10 201 84 85	3012 NC Rotterdam
E-mail:	info@lrqa.nl	The Netherlands

Hoewel andere certificatie-instellingen hier nog nauwelijks mee actief zijn, kan desgevraagd wel nadere informatie over de toepasbaarheid van deze normen worden gegeven.

Tot slot kan nog worden meegedeeld dat mede vanwege de affaire bij Tredin B.V. het aspect privacy nadrukkelijker onderwerp van onze audits is geworden.

Indien nadere informatie is gewenst, verneem ik dat graag.

Hoogachtend,

A handwritten signature in black ink, appearing to be 'P.G. Cornelissen', written over a horizontal line.

P.G. Cornelissen
Manager LRQA Nederland
Lloyd's Register Nederland B.V.

A member of the Lloyd's Register Group.

A company registered at the Chamber of Commerce in Rotterdam under number 24247943. Our general terms and conditions LRQA shall apply to any agreement.
This document is subject to [LRQA's network of offices worldwide](#)