D34 (= bylage van D33)

Concept-Beleidsnotitie Informatiebeveiligingsbeleid CSZ versie 2.0

Toezichttaken CSZ

Het CSZ Het College sanering zorginstellingen (CSZ) is een zelfstandig bestuursorgaan (ZBO) dat namens de minister van Volksgezondheid, Welzijn en Sport (VWS) een aantal taken uitvoert.

Het huidige takenpakket van het CSZ bestaat uit het toezicht op :

- Vervreemding onroerende zaken

Wanneer een zorginstelling terreinen, gebouwen of delen daarvan wil verkopen, verhuren of aan een beperkt recht onderwerpen, is de directie of de Raad van Bestuur van een instelling wettelijk verplicht dit bij het CSZ te melden. Als het CSZ besluit dat goedkeuring vereist is, vindt toezicht plaats op het verkoopproces dat moet leiden tot een marktconforme opbrengst. Doelstelling van het toezicht is om te voorkomen dat geld "weglekt" uit de zorg. Er wordt momenteel aan circa 600 casus gewerkt.

- Saneringsregeling zorginstellingen

Bij een intrekking of beperking van de toelating van een instelling houdt het CSZ toezicht op het saneringsproces. Het CSZ kan subsidie geven die (deels) voorziet in de financiële gevolgen van deze beperking of intrekking. Vrijgevestigde medische beroepsbeoefenaren kunnen subsidie krijgen om de teruggang in hun inkomen op te vangen tijdens de periode die voorafgaat aan de beperking of intrekking van de toelating. Voorwaarde voor aanmelding is een beslissing omtrent de toelating ("sluitingsbeslissing") van de minister van VWS. Hoewel de saneringsregeling nog bestaat, zijn er de afgelopen jaren geen sluitingsbeslissingen meer genomen. Het College behandelt nog lopende zaken. Het gaat op dit moment om nog één lopende casus

- Saneringsregeling ambulancehulpverlening

Bij het intrekken van een vergunning van een ambulancedienst en bij het wijzigen of opheffen van de vestigingsplaats van een Centrale Post voor het Ambulancevervoer kon het CSZ subsidie verstrekken om de financiële gevolgen geheel of gedeeltelijk op te vangen. Deze saneringsregeling is beëindigd. Lopende zaken worden door het College sanering afgehandeld. Het gaat op dit moment om nog één lopende casus

- Overige werkzaamheden

De minister of staatssecretaris van VWS kan het College sanering vragen bijzondere werkzaamheden uit te voeren of een regiefunctie te vervullen. Tot circa 10 jaar geleden is een aantal keren is onderzoek uitgevoerd bij instellingen in financiële problemen. De expertise van het CSZ heeft zich de laatste jaren steeds meer toegespitst op vastgoed. Deze expertise is beschikbaar voor het uitvoeren van onderzoeken voor het ministerie van VWS of voor andere ZBO's.

Organisatie CSZ

Het bestuur van het CSZ bestaat uit twee personen die tevens de Raad van Bestuur van de NZa vormen. Het secretariaat van het CSZ bestaat uit 5 personen die in dienst zijn van de NZa. Het CSZ maakt voor de uitvoering van de toezichttaken gebruik van zogenoemde gemachtigden die per casus worden aangewezen en ingehuurd. De gemachtigden zijn deskundigen op het gebied van (zorg-) vastgoed. De gemachtigden adviseren het College over de onroerend goed transacties (open en

transparante vervreemdingsproces en de marktconformiteit van de prijs). Het aantal gemachtigden is momenteel 10.

De uitvoeringsorganisatie van het CSZ, de casusbehandeling is in verregaande mate gestandaardiseerd. Er is een casusregistratie- en workflow-systeem.

Uitgangspunten informatiebeveiligingsbeleid CSZ

Deze beleidsnotitie is geschreven op basis van de Baseline informatiebeveiliging Overheid (BIO).

De Baseline informatiebeveiliging overheid (BIO) is bedoeld om de (significante) risico's en bedreigingen te onderkennen die schade met zich meebrengen als gevolg van het (tijdelijk) niet beschikbaar zijn van (informatie-) systemen, het niet integer zijn van informatie en het in verkeerde handen vallen van informatie. De BIO bevat tevens een overzicht van te nemen specifieke beheersmaatregelen.

De BIO is opgesteld voor generieke schades en bedreigingen bij de Rijksoverheid en de passende maatregelen hiervoor genomen kunnen worden. Het zogenoemde basis beveiligingsniveau (BBN).

Er worden 3 niveaus BBN onderscheiden. Het CSZ herkent zich in BBN niveau 2 omdat er met bedrijfsgevoelige informatie wordt gewerkt en mogelijke incidenten, mede vanwege het feit dat de Raad van bestuur de NZa het Collegebestuur vormt, tot bestuurlijke commotie kunnen leiden.

BBN 3 is niet van toepassing omdat het College sanering geen departementaal vertrouwelijke informatie verwerkt waarbij weerstand geboden moet worden tegen een statelijke dreiging/actoren.

De strategische doelen van het informatiebeveiligingsbeleid

Het CSZ onderkent de volgende strategische doelen voor het informatiebeveiligingsbeleid.

-het managen van de risico's die gelden bij informatiebeveiliging, die betrekking hebben op: beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening.

Hieronder wordt onder verstaan:

-het correct registreren, archiveren en -beveiligen van vertrouwelijke gegevens zoals persoons-/bedrijfsgevoelige gegevens van burgers, medewerkers en zorginstellingen;

-adequate bescherming van bedrijfsmiddelen;

-het waarborgen van veilige informatiesystemen;

-het beschermen van kritieke bedrijfsprocessen;

-het beheersen van risico's van menselijk gedrag;

-het voorkomen van ongeautoriseerde toegang c.q. het beheersen van de toegang tot informatiesystemen;

-het adequaat reageren op incidenten;

-het waarborgen van de naleving van dit beleid.

De governance mbt het informatiebeveiligingsbeleid

-Het bestuur van College is eindverantwoordelijk voor de informatiebeveiliging;

-De Chief Information Officer (CIO) is eindverantwoordelijk voor het informatiebeveiligingsbeleid. Deze notitie betreft een vervolgstap, een actualisatie van het informatiebeveiligingsbeleid zoals dat in februari 2020 voor het eerst is vastgesteld, aangeduid als informatiebeveiligingsbeleid 1.0. De CIO is tevens verantwoordelijk voor de onafhankelijke toetsing op de naleving van het informatiebeleid;

-De verantwoordelijkheid voor de uitvoering ligt bij de manager CSZ;

-Het informatiebeveiligingsbeleid wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, incidenten en actualisatie van risicoanalyses;

-Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging.

-Het CSZ stelt jaarlijks een (geactualiseerd) informatiebeveiligingsbeeld op.

Significant risico en beheersmaatregelen

Gelet op het werkproces met betrekking tot de toezichttaken van het CSZ en het feit dat het bestuur van het CSZ uit dezelfde personen bestaat als het bestuur van de NZa onderkent het CSZ het volgende significante risico dat beheerst moeten worden.

Het niet correct registreren, archiveren en beveiligen van privacy- en bedrijfsgevoelige gegevens

De belangrijkste beheersmaatregelen op basis van de BIO en de risico-analyse liggen op het terrein van:

a-De bewustwording van medewerkers met betrekking tot informatiebeveiliging;

b-De borging van de continuïteit van het casus- en workflowsysteem;

c-Het voorkomen van ongeautoriseerde toegang tot het informatiesysteem waaronder ook wordt verstaan de (fysieke) archiefruimte mbt de dossiers;

d-Het inregelen van de Plan Do Check act cyclus in termen van een uitvoeren van een periodieke risico-analyse, de verificatie van de getroffen maatregelen en de eventuele aanpassing van de getroffen maatregelen met als resultante een informatiebeveiligingsbeeld (zie bijlage), waar uit moet blijken dat de ín opzet' (op papier) getroffen maatregelen 'bestaan' en 'werken'. In het informatiebeveiligingsbeeld zijn de belangrijkste nog op te pakken) aandachtspunten opgenomen.

Het College sanering heeft voor het monitoren van de uitvoering van het informatiebeveiligingsbeleid een PDCA (Plan-DO-Check-Act) Cyclus ingericht met daarin als belangrijke elementen:

- het periodieke overleg met de ICT-leverancier die de prestaties van het geautomatiseerde gegevensverwerkende systeem (kantoorautomatisering, Easy, Acces) van het College sanering monitort;
- het jaarlijks actualiseren van de risicoanalyse;
- het bijhouden van een incidentenregistratie;
- het jaarlijks actualiseren van het informatiebeveiligingsbeeld;

- het in voorkomende gevallen treffen van maatregelen naar aanleiding van knelpunten, incidenten, de jaarlijkse risicoanalyse, het periodieke overleg met de ICT-leverancier en bevindingen naar aanleiding van (eventueel) uitgevoerde externe audits op de uitvoering van het informatiebeveiligingsbeleid.