Nota van toelichting

1. Algemeen

Dit besluit wijzigt het Tuchtrechtbesluit BIG en biedt daarmee regels voor vrijwillig elektronisch procederen in het tuchtrecht in de gezondheidszorg. In een wijziging van de Wet op de beroepen individuele gezondheidszorg (hierna: wijziging Wet BIG[1]) is, naast het opnemen van de medisch hulpverlener acute zorg en klinisch fysicus in de lijst van registerberoepen, de mogelijkheid om langs elektronische weg te procederen bij de tuchtcolleges expliciet opgenomen in de wet. Dit besluit geeft uitwerking aan de artikelen 64b en 64d van de Wet BIG, door onder andere te bepalen aan welke eisen een digitaal systeem voor gegevensverwerking (hierna: het systeem) moet voldoen dat door de tuchtcolleges voor de gezondheidszorg (hierna: de tuchtcolleges) wordt gebruikt voor verkeer langs elektronische weg. Benadrukt wordt dat de keuze voor het procederen langs elektronische weg aan de procespartij of procesvertegenwoordiging is. Het blijft dus mogelijk om een klacht op papier in te dienen. Echter, als een procespartij of procesvertegenwoordiging gebruik wil maken van de mogelijkheid tot elektronisch procederen, voorziet dit besluit in een regelgevend kader waaraan de tuchtcolleges moeten voldoen.

Achtergrond van het besluit
Aanleiding voor de hiervoor genoemde wijziging van de Wet BIG was een reeks van datalekken met fysieke postbezorging en de daarmee gepaard gaande kosten om de datalekken te mitigeren. Bovendien is er in toenemende mate sprake van digitalisering in de communicatie tussen burger en overheid. Inmiddels zijn regels met betrekking tot digitalisering opgenomen in verschillende wetten zoals de Wet modernisering elektronisch bestuurlijk verkeer, de Wet tot wijziging van het Wetboek van Burgerlijke Rechtsvordering en de Algemene wet bestuursrecht in verband met vereenvoudiging en digitalisering van het procesrecht. Het tuchtrecht voor de gezondheidszorg valt echter niet onder het toepassingsbereik van deze wetten. Zo zijn de tuchtcolleges geen bestuursorganen, waardoor de Wet modernisering elektronisch bestuurlijk verkeer en de Algemene wet bestuursrecht niet van toepassing zijn. Daarnaast kwalificeert het tuchtrecht voor de gezondheidszorg niet als civiel recht omdat er geen sprake is van een burgerlijke procedure, waardoor ook het Wetboek van Burgerlijke Rechtsvordering niet van toepassing is. Het tuchtrecht in de gezondheidszorg heeft zijn eigen gesloten stelsel van procesrecht in de Wet BIG en het Tuchtrechtbesluit BIG om de unieke positie van medische kwaliteitsrechtspraak te waarborgen. Regels over digitalisering van het tuchtproces moeten daarom in de Wet BIG en in het Tuchtrechtbesluit BIG worden opgenomen.

Het doel van digitalisering van het tuchtproces is burgers laagdrempelig in te staat te stellen hun klacht langs elektronische weg in te dienen, de daaropvolgende schriftelijke procedure langs elektronische weg te voeren en de uitspraak elektronisch te ontvangen. Het gaat hier slechts om de mogelijkheid en niet om de verplichting tot elektronisch procederen. De burger heeft zelf de keuze tussen het volgen van de elektronische weg of de papieren weg. Hier is voor gekozen om de toegang tot de tuchtrechter blijvend mogelijk te maken voor partijen die onvoldoende expertise hebben om gebruik te maken van het internet of mobiele apps, en daarnaast digitaal toegang tot de tuchtrechter mogelijk te maken.

Bij de uitwerking van dit besluit is voor zover van toepassing, aansluiting gezocht bij het Besluit elektronisch procederen (hierna: Bep) voor het civiele recht en het bestuursrecht. Voor een antwoord op de vraag aan welke betrouwbaarheids- en zorgvuldigheidseisen het systeem moet voldoen, is immers niet relevant of er geprocedeerd wordt in een bestuursrechtelijke, civielrechtelijke, of binnen het tuchtrecht voor de gezondheidszorg. Het maakt evenmin verschil of de procespartijen verplicht zijn om gebruik te maken van een digitaal systeem, zoals in het bestuursrecht of civiele recht aan de orde kan zijn, of dat hiervan vrijwillig gebruik wordt gemaakt, zoals in het tuchtrecht voor de gezondheidszorg: een systeem dat gebruikt wordt voor elektronisch procederen moet ten alle tijden betrouwbaar zijn en waarborgen bieden voor een zorgvuldige procesvoering.

[1] Kamerstukken II 2025/26, 36 832, nr. 2

Het procederen langs elektronische weg omvat het verzenden en ontvangen van berichten en stukken in tuchtrechtelijke procedures via een aangewezen systeem aan en met de in artikel 2 van het Tuchtrechtbesluit BIG genoemde tuchtcolleges. In deze berichten kunnen processtukken en overige voor het dossier relevante communicatie, zoals het klaagschrift en andere correspondentie, worden uitgewisseld. Het besluit ziet op het verkeer tussen de tuchtcolleges en de bij een procedure betrokken partijen.

De verwachting is dat voor klagers, BIG-geregistreerde beroepsbeoefenaren, en de tuchtcolleges het procederen langs elektronische weg zal bijdragen aan een betere, snellere en veiligere communicatie. Bovendien is de verwachting dat elektronisch procederen leidt tot een eenvoudigere en snellere verwerking van aangeleverde stukken, en tot een efficiëntere en meer duurzame werkwijze bij de administraties van de tuchtcolleges. De tuchtcolleges zijn bezig met de realisatie van het systeem. In de eerstvolgende fase kunnen partijen digitaal procederen. Het digitaal indienen van stukken zal naar verwachting in de loop van 2027 mogelijk zijn.

Grondslagen voor dit ontwerpbesluit
De grondslagen voor dit besluit zijn opgenomen in de artikelen 64b en 64d van paragraaf 3a van hoofdstuk VII van de Wet BIG. Deze nieuwe paragraaf van de Wet BIG bepaalt op welke wijze elektronisch verkeer met de regionale tuchtcolleges en het centrale tuchtcollege kan plaatsvinden. Opgenomen is onder meer dat daar waar het tuchtrecht bepaalt dat handelingen schriftelijk geschieden, hieraan langs elektronische weg kan worden voldaan[2]. Bovendien kan een voorzitter bepalen dat een digitaal ingezette procedure met papieren stukken wordt voortgezet[3]. Ook is de grondslag opgenomen dat bij algemene maatregel van bestuur nadere regels gesteld worden over het elektronisch verkeer[4]. Deze regels worden nader uitgewerkt in dit besluit.

2. Regeldruk, gevolgen voor de tuchtcolleges en financiële gevolgen

De lasten die gepaard gaan met procederen langs elektronische weg hangen samen met de waarborgen die het tuchtrecht voor de gezondheidszorg dient te bieden voor een efficiënte procesvoering. Dit besluit roept geen nieuwe informatieverplichtingen in het leven: het biedt enkel de ruimte op vrijwillige basis elektronisch procederen in het tuchtrecht voor de gezondheidszorg mogelijk te maken. Vanwege dit bijzondere karakter van deze regels worden ze, evenals in het Bep en in het Besluit grondslag verplicht elektronisch procederen in civiele zaken, niet als regeldruklasten aangemerkt.

Personen die gebruik willen maken van de mogelijkheid voor procederen langs elektronische weg, dienen te beschikken over een authenticatiemiddel[5] dat voldoet aan artikel 3a van dit besluit. Daarnaast dienen zij te beschikken over de toegang tot een computer of een ander elektronisch apparaat. Zowel professionele partijen als particulieren beschikken veelal over dergelijke voorzieningen, waardoor hier geen extra kosten uit zullen voortvloeien. Elektronisch procederen kan voor partijen ook tot besparingen leiden doordat sneller kan worden gewerkt en er minder of geen kopieer- of frankeerkosten nodig zijn. Daarnaast kunnen partijen makkelijker toegang krijgen tot hun dossier in het systeem. Voor degenen die daar geen gebruik van kunnen of willen maken, blijft de mogelijkheid van procederen langs papieren weg bestaan. Daardoor kunnen stukken via de post ingediend worden bij de tuchtcolleges, waarna ze worden in gescand en toegevoegd aan het systeem. USB-sticks en bestandtypes die niet in te scannen zijn, worden per koerier aan de tuchtcolleges gezonden.

Dit besluit heeft geen financiële gevolgen: het besluit stelt regels over elektronisch procederen, maar het verplicht daar niet toe. De kosten voor de uitvoering van de digitalisering bij de tuchtcolleges liggen bij Eenheid Secretariaten voor de Tuchtcolleges voor de Gezondheidszorg en Toetsingscommissies Euthanasie (hierna: ESTT).

[2] Artikel 64a, vierde lid Wet BIG.
[3] Artikel 64a, vijfde lid Wet BIG.
[4] Artikel 64d Wet BIG.
[5] Op het moment van schrijven van het conceptbesluit gaat het om DigiD en eHerkenning, zie ook de artikelsgewijze toelichting bij artikel 3a.

3. Advies en consultatie
PM (Internetconsultatie, ATR, CIBG, IGJ)

4. Verwerking persoonsgegevens
De tuchtcolleges verwerken persoonsgegevens in overeenstemming met de Algemene verordening gegevensbescherming, de Uitvoeringswet Algemene verordening gegevensbescherming en de Archiefwet. Doel van deze gegevensverwerking is het zorgvuldig en rechtmatig uitvoeren van de tuchtrechtelijke taak van de tuchtcolleges. De verwerking van persoonsgegevens is noodzakelijk om het tuchtrecht goed te laten functioneren, met respect voor zowel rechtsbescherming als privacy. Dit doel is niet anders bij procederen langs de elektronische weg. Alleen de wijze waarop de gegevens bij de tuchtcolleges terechtkomen, wijzigt met het procederen langs elektronische weg. Voor de toegang tot het systeem wordt gebruikgemaakt van elektronische identificatiemiddelen, zoals DigiD en eHerkenning. In het geval van DigiD wordt het BSN uitsluitend gebruikt in het kader van de authenticatie; het DigiD wordt niet opgenomen in het procesdossier. De inrichting en het beheer van het systeem, waaronder de toegangsvoorziening, vallen onder de verantwoordelijkheid van ESTT.

ESTT is een directie binnen het Ministerie van Volksgezondheid, Welzijn en Sport (hierna: VWS). ESTT draagt zorg voor het faciliteren van juridische en administratieve dienstverlening aan de onafhankelijke tuchtcolleges voor de gezondheidszorg en toetsingscommissies euthanasie. De tuchtcolleges zijn in verband hiermee niet apart in de Wet digitale overheid (hierna: Wdo) opgenomen, omdat het Ministerie van VWS als proces- en systeemeigenaar van het systeem onder deze wet valt. ESTT vervult daarbij, op basis van een mandaatbesluit, de rol van verwerkingsverantwoordelijke namens deze onderdelen voor zover het de verwerking van persoonsgegevens in het kader van de uitvoering van de ondersteunende processen betreft.

Artikelsgewijze toelichting

Artikel I

Artikel 3

Eerste lid

Het eerste lid van dit artikel bepaalt dat elektronisch procederen via het systeem mogelijk is als in het betreffende procesreglement van de tuchtcolleges de mogelijkheid daartoe is opengesteld. Een dergelijk systeem omvat een voorziening waarmee in medisch tuchtrechtelijke procedures berichten en stukken elektronisch uitgewisseld kunnen worden tussen een procespartij en de tuchtcolleges. Dit systeem dient vervolgens aangewezen te worden in het al bestaande procesreglement dat gepubliceerd is op de website van de tuchtcolleges. De drie regionale tuchtcolleges stellen gezamenlijk één procesreglement vast, en het centraal tuchtcollege stelt een eigen procesreglement vast. Dus, hoewel er formeel gezien sprake is van twee verschillende procesreglementen, ligt het in de rede dat afstemming plaatsvindt tussen de tuchtcolleges over het aan te wijzen systeem, waardoor in beide procesreglementen hetzelfde systeem wordt opgenomen. Dit bevordert de rechtszekerheid, toegankelijkheid en werkbaarheid voor zowel procespartijen als de tuchtcolleges, en draagt tevens bij aan de integriteit, beschikbaarheid en vertrouwelijkheid van de van de gegevensverwerking.

Tweede lid

Het tweede lid van dit artikel bevat de eisen waaraan het systeem moet voldoen. Deze eisen zijn gelijkluidend aan de eisen in artikel 3 van het Besluit elektronisch procederen, waarbij het gaat om doelbepalingen: het artikellid schrijft geen specifieke methoden of technieken voor, maar is erop gericht gebruikers van het systeem waarborgen te bieden met betrekking tot de zorgvuldigheid en betrouwbaarheid van het systeem.

Tweede lid, onderdeel a

De gebruiker is degene die inlogt in het systeem. De gebruiker is een procespartij, een (niet-)juridisch gemachtigde van een procespartij, of een medewerker van de tuchtcolleges (een interne gebruiker zoals een griffier of een voorzitter). De gebruiker kan inloggen om stukken toe te voegen aan het dossier, te verzenden of (als er een digitaal dossier is) te raadplegen.

De identificatie van een externe gebruiker die via een gebruikersinterface (zoals een webportaal of app) toegang heeft tot het systeem, heeft betrekking op de natuurlijke persoon die toegang wenst tot het systeem, ook indien deze namens een rechtspersoon optreedt. Het systeem moet de tuchtcolleges dus in staat stellen eenieder die via een gebruikersinterface toegang verkrijgt te identificeren (wie is de gebruiker?), diens identiteit te kunnen controleren (authentiseren: nagaan of de gebruiker is wie hij zegt te zijn), alsmede te autoriseren (vaststellen waar de gebruiker toe gerechtigd is).

Wordt via een systeemkoppeling toegang verkregen dan dient het systeem van de tuchtcolleges bovendien te kunnen controleren of dit inderdaad het systeem betreft waarvan is geoordeeld dat het kan worden gekoppeld. Voor de systeemkoppeling vindt de authenticatie plaats, en wordt de autorisatie afgestemd op het gebruiksdoel. De koppeling wordt daarbij volgens geldende standaarden en afspraken veilig geïmplementeerd, waaronder ondertekening van het bericht en versleuteling van de inhoud van het bericht en de verbinding. Het gekoppelde systeem is dan de gebruiker in de zin van onderdeel a.

Tweede lid, onderdeel b

Als een procespartij of procesvertegenwoordiger via een gebruikersinterface (bijvoorbeeld via een webportaal of app) toegang krijgt tot het systeem, spreken we over externe gebruikers. Het begrip procespartij duidt enerzijds op de indiener van het klaagschrift, zoals bepaald in artikel 65, eerste lid van de Wet BIG, waardoor de tuchtrechtelijke procedure aanhangig wordt gemaakt. Dit kunnen een rechtstreeks belanghebbende, degene die aan de beklaagde een opdracht heeft verstrekt, degene bij wie of het bestuur van een instelling waarbij beklaagde werkzaam is, en een inspecteur van de Inspectie Gezondheidszorg en Jeugd (hierna: IGJ) zijn. Anderzijds is sprake van de beklaagde als procespartij. Met procesvertegenwoordiger wordt de raadsman, dan wel een andere gemachtigde bedoeld.

Dus, als er sprake is van een procespartij of procesvertegenwoordiger die via een gebruikersinterface (zoals een webportaal of app) toegang verkrijgt tot het systeem, geldt niet alleen identificatie op grond van onderdeel a, maar ook authenticatie op grond van onderdeel b.

Voor toegang tot het systeem via een systeemkoppeling geldt artikel 3, derde lid. De authenticatie van de individuele gebruiker die via een systeemkoppeling gebruik maakt van het aangewezen systeem, vindt daarbij plaats door het te koppelen systeem. Voor een nadere toelichting over de authenticatie zelf, wordt verwezen naar de artikelsgewijze toelichting bij artikel 3a.

De vereisten voor toegang van interne gebruikers, dat wil zeggen een voorzitter, secretaris, of een andere medewerker van de tuchtcolleges, worden niet geregeld in dit besluit. Deze personen zullen toegang verkrijgen via hun werkplek. De toegangscontrole (identificatie, authenticatie en autorisatie) van interne gebruikers vindt plaats bij het inloggen in de digitale werkomgeving van de tuchtcolleges.

Tweede lid, onderdeel c

De indiener is de persoon die de proceshandeling verricht. De gebruiker van het systeem en de indiener kunnen een en dezelfde persoon zijn, maar dit hoeft niet. Zo kan het bijvoorbeeld voorkomen dat de secretariaatsmedewerker van de raadsman de stukken van de raadsman namens hem indient. De secretariaatsmedewerker is in dat geval de onder a bedoelde gebruiker, die inlogt met zijn of haar gemachtigdenpas om stukken afkomstig van de raadsman in te dienen. De raadsman is in dat geval degene die wordt beschouwd als indiener als bedoeld onder onderdeel c. Het feit dat een raadsman of een andere gemachtigde zelf ook namens een cliënt respectievelijk volmachtgever optreedt, maakt dit niet anders. Dus, degene die de proceshandeling verricht, wordt beschouwd als de indiener in de zin van onderdeel c.

Met het bericht in de zin van dit onderdeel van artikel 3, tweede lid, van het besluit wordt een soort digitale envelop bedoeld, waarmee verzoeken, mededelingen, processtukken of andere communicatie (dus de inhoud van de envelop) worden verzonden. Middels één bericht kunnen dus

meerdere stukken worden ingediend, bijvoorbeeld een dagvaarding of beroepsschrift met bijlagen. De eisen die aan het verzenden van een bericht via het systeem worden gesteld in de volgende onderdelen, gelden eveneens voor in het bericht vervatte stukken en andere communicatie.

Tweede lid, onderdeel d

Het systeem moet controle mogelijk maken op de integriteit van het via het systeem verzonden bericht, en daarmee ook van de in het bericht vervatten stukken. Het bericht en de daarin vervatten stukken dienen na indiening volledig en ongewijzigd te zijn en blijven. Een bericht heeft immers een definitieve status en mag niet worden gewijzigd.

Tweede lid, onderdeel e

Het systeem moet controle mogelijk maken van het moment van ontvangst en verzending van berichten door de tuchtcolleges. Het tijdstip van ontvangst en verzending van het bericht door het systeem is tevens het tijdstip van ontvangst en verzending van de in het bericht vervatte stukken. Zie voor een nadere toelichting de artikelsgewijze toelichting bij artikel 3b.

Tweede lid, onderdeel f

Toegang tot de berichten in het systeem en daarmee tot de inhoud daarvan dient enkel te worden verkregen door degene die daartoe gerechtigd is. De controle op de autorisatie vormt, na identificatie en eventueel authenticatie ingeval van een externe gebruiker, het sluitstuk van het proces tot toegangsverlening tot het systeem. Als het systeem ook voorziet in de toegang tot een digitaal dossier (bestaande uit de procesinformatie, uitgewisselde berichten en hun inhoud), geldt de eis om de berichten uitsluitend toegankelijk te maken voor geautoriseerde gebruikers ook voor de toegang tot dit digitaal dossier.

Tweede lid, onderdeel g

Het systeem moet controle mogelijk maken op de verschoonbaarheid van een termijnoverschrijding (zie artikel 3c van dit besluit), waardoor het noodzakelijk is na te kunnen gaan wanneer een verstoring heeft plaatsgevonden. Onder een verstoring wordt zowel gepland onderhoud als een technisch mankement verstaan. Zie voor een nadere toelichting de artikelsgewijze toelichting bij artikel 3c.

Derde lid

Via een systeemkoppeling kunnen digitale systemen van bepaalde organisaties, zoals bijvoorbeeld het Centraal Informatiepunt Beroepen Gezondheidszorg (hierna: CIBG), de IGJ, de Rijksdienst voor Informatiehuishouding (hierna: RvIHH), de Rijksdienst voor Identiteitsgegevens (hierna: RvIG), Logius, SSC-ICT, en DICTU, worden gekoppeld aan het systeem van de tuchtcolleges. Er wordt pas overgegaan tot het koppelen van systemen als er voldoende waarborgen zijn dat het te koppelen systeem ten minste even betrouwbaar is als het aangewezen systeem van de tuchtcolleges. Om dit te borgen zullen er eisen worden gehanteerd waaraan een te koppelen systeem dient te voldoen. Deze aansluitvoorwaarden worden door de tuchtcolleges nader uitgewerkt in een technisch reglement.

Na koppeling van het systeem ziet de authenticatie door het systeem van de tuchtcolleges strikt genomen louter op de vaststelling of het inderdaad om het systeem gaat dat gekoppeld mag worden (authenticatie van het systeem). De systeemkoppeling authenticeert de applicatie, en autorisatie aan gebruikers vindt plaats op basis van de identiteit en rechten van de gebruiker. Indien vanuit de systeemkoppeling toegang wordt verstrekt tot het systeem van de tuchtcolleges, dan geldt artikel 3a van het besluit. Het betrouwbaarheidsniveau van het te koppelen systeem wordt voor een groot deel bepaald door het betrouwbaarheidsniveau van de authenticatiemiddelen die worden gebruikt om toegang te verschaffen tot het te koppelen systeem, maar staat daaraan niet automatisch gelijk. Het gaat om het totaal aan maatregelen die zijn getroffen om te waarborgen dat de communicatie betrouwbaar en vertrouwelijk verloopt.

Vierde lid

De grosse (een in executoriale vorm opgesteld afschrift van een uitspraak) is uitgezonderd van elektronische verzending omdat het in een elektronische omgeving vooralsnog niet mogelijk is te garanderen dat er slechts één authentieke grosse bestaat: ieder afschrift van een elektronisch

document is identiek. Partijen kunnen uiteraard wel langs elektronische weg kennisnemen van de uitspraak in niet-executoriale vorm.

Artikel 3a

Dit artikel schrijft voor waaraan een middel moet voldoen waarmee een gebruiker als bedoeld in artikel 3, tweede lid, onderdeel b, zich authenticeert om toegang te verkrijgen tot het systeem en toegang verkrijgt via een gebruikersinterface, bijvoorbeeld via een webportaal. Dit geldt dus enkel voor externe gebruikers, te weten de procespartij, procesvertegenwoordiger, of (college)-ledenberoepsgenoten. Voor interne gebruikers, te weten een voorzitter, secretaris, of een andere medewerker van de tuchtcolleges, gelden deze authenticatievereisten dus niet.

De eisen neergelegd in dit artikel vloeien voort uit het voor de elektronische dienstverlening benodigde betrouwbaarheidsniveau. De indeling in betrouwbaarheidsniveaus volgt de indeling uit Verordening (EU) 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (hierna: de eIDAS-verordening)[6]. De eIDAS-verordening geeft een wettelijk kader voor het bepalen van het betrouwbaarheidsniveau voor digitale overheidsdiensten. De verordening onderkent drie betrouwbaarheidsniveaus: laag, substantieel en hoog. Voor elektronisch procederen in het tuchtrecht voor de gezondheidszorg wordt zo veel mogelijk aangesloten bij (ten minste) het betrouwbaarheidsniveau substantieel[7]. Dit houdt onder meer in dat bij de aanvraag van het middel daadwerkelijk vastgesteld moet worden dat de gebruiker een geldig officieel document bezit met dezelfde identiteitsgegevens die gecontroleerd kunnen worden in een basisregistratie. Deze controle mag uitbesteed worden of op afstand plaatsvinden.

Artikel 3a stelt dat het middel dat wordt aangewezen in het procesreglement moet voldoen aan de volgende eisen:

a. het middel is afgegeven door de overheid of door een onder toezicht van de Minister van Binnenlandse Zaken en Koninkrijksrelaties (hierna: BZK) staande organisatie; en
b. het middel gebruikt tweefactorauthenticatie of voldoet ten minste aan het betrouwbaarheidsniveau substantieel.

Ad a. Met een ‘door de overheid afgegeven middel’ wordt op het moment van inwerkingtreding van dit besluit DigiD bedoeld. Dit betekent dat de gebruiker via diens DigiD kan inloggen. Mocht DigiD in de toekomst wijzigen in een ander instrument, kwalificeert deze opvolger van DigiD als ‘het middel afgegeven door de overheid’ bedoeld in dit onderdeel. Met een ‘onder toezicht van de Minister van BZK staande organisatie’ wordt gedoeld op een organisatie waarvan door de Minister van BZK is bepaald dat deze identificatiemiddelen mag afgeven[8]. Deze identificatiemiddelen voor ondernemers worden aangeduid als eHerkenning. Op het moment van inwerkingtreding van dit besluit zijn er zes commerciële leveranciers van eHerkenning op betrouwbaarheidsniveau substantieel, die onder het vorenbedoelde toezicht vallen[9]. eHerkenning hanteert vijf betrouwbaarheidsniveaus, waarbij eHerkenning 4 gelijkstaat aan het betrouwbaarheidsniveau substantieel.

Ad b. Als type middel is tweefactorauthenticatie of een middel dat voldoet aan het betrouwbaarheidsniveau van ten minste substantieel vereist. Door de eis dat het middel moet uitgaan van tweefactorauthenticatie of moet voldoen aan het betrouwbaarheidsniveau van ten minste substantieel, wordt voor alle middelen de ondergrens bepaald. Tweefactorauthenticatie houdt in dat er twee verschillende authenticatiemethoden worden gebruikt, bijvoorbeeld iets wat

---

[6] De indeling in betrouwbaarheidsniveaus geldt in de eIDAS-verordening enkel voor authenticatiemiddelen. In lijn met de *Handreiking voor overheidsorganisaties. Betrouwbaarheidsniveaus voor digitale dienstverlening* hanteert dit besluit de indeling in betrouwbaarheidsniveau ook voor de dienst zelf (i.c. elektronisch procederen).
[7] Bijzonder vertrouwelijke stukken waarvoor betrouwbaarheidsniveau hoog zou gelden, kunnen buiten het systeem op papier worden ingediend.
[8] Als eigenaar van het afsprakenstelsel voor elektronische toegangsdiensten, is de Staatssecretaris van BZK tevens toezichthouder. Om de rollen van eigenaar en toezichthouder zo veel mogelijk te scheiden, is een Commissie van Deskundigen ingesteld door de Minister van Economische Zaken (Besluit van de Minister van Economische Zaken van 14 april 2016, nr. WJZ/16008896, tot instelling van de Commissie van Deskundigen voor het toezicht op het ETD-stelsel).
[9] Zie eHerkenning | Leveranciersoverzicht.

de gebruiker weet (een wachtwoord of code) en iets wat de gebruiker heeft (een pasje of token). Er moet een controle plaatsvinden om te waarborgen dat degene die gebruik maakt van het middel ook degene is aan wie het middel is uitgegeven zodat de gebruiker beschermd is tegen misbruik van zijn gegevens. Het middel moet zo ontworpen zijn dat het alleen onder controle van de gebruiker gebruikt kan worden. Het mag niet mogelijk zijn dat het per ongeluk of ongemerkt door een ander kan worden gebruikt. Bij het betrouwbaarheidsniveau substantieel geldt daarnaast dat sprake moet zijn van dynamische authenticatie. De (cryptografische) gegevens voor de authenticatie veranderen bij ieder gebruik. Dit biedt extra bescherming tegen fraudeurs die gegevens willen stelen en hergebruiken. Een voorbeeld van dynamische authenticatie zijn tokens die wachtwoorden voor eenmalige gebruik aanmaken (one-time password tokens).

De tuchtcolleges hoeven alleen identificatiemiddelen te accepteren die door hen zijn aangewezen in het procesreglement.

Artikel 3b

Dit artikel bepaalt wanneer een bericht als ontvangen en verzonden door (het secretariaat van) het tuchtcollege wordt beschouwd. Als tijdstip van ontvangst door het tuchtcollege geldt het tijdstip waarop het bericht het daartoe aangewezen systeem voor gegevensverwerking heeft bereikt. Als tijdstip van verzending door (het secretariaat van) het tuchtcollege geldt het tijdstip waarop het bericht toegankelijk wordt voor de geadresseerde van het bericht in het daartoe aangewezen systeem van voor gegevensverwerking[10]. Een aanvullende ontvangstbevestiging verzonden door het tuchtcollege wordt niet noodzakelijk geacht, omdat de indiener via het systeem kan zien of en wanneer zijn bericht verzonden is, en wanneer het ontvangen is door het tuchtcollege.

Artikel 3c

Dit artikel bepaalt dat als een stuk wordt ingediend door een externe gebruiker waarvan de identiteit is geauthentiseerd bij de toegangsverlening tot het systeem, het stuk geldt als ondertekend door die persoon.

Artikel 3d

Dit artikel bepaalt hoe omgegaan moet worden met een verstoring van de toegang tot het in het procesreglement aangewezen systeem. Een partij die elektronisch procedeert, ongeacht of dit op grond van een verplichting of op vrijwillige basis geschiedt, moet erop kunnen vertrouwen dat zij gebruik kan maken van het systeem. Het blijft daarbij de verantwoordelijkheid van partijen om berichten tijdig in te dienen. Dit artikel ziet uitsluitend op een verstoring op de laatste dag van een termijn. De bepaling is daardoor concreter geformuleerd dan de algemene regeling in de Awb[11] over termijnoverschrijding, die uitsluitend in het bestuursrecht van toepassing is, terwijl het onderhavige artikel geldt in medisch tuchtrechtelijke procedures.

Voorts geldt deze bepaling enkel als de verstoring niet aan de indiener is toe te rekenen. Dat is in beginsel het geval als de verstoring plaatsvindt door een oorzaak in het systeem. De tuchtcolleges zullen registreren («loggen») of er storingen in of van het systeem zijn en hoe lang die zich hebben voorgedaan. Een overzicht van deze storingen zal via de website beschikbaar worden gesteld. Rechtzoekenden kunnen hierdoor onderbouwen of hun termijnoverschrijding verschoonbaar is. Publicatie van het moment van het verholpen zijn van een storing op bijvoorbeeld de website van de tuchtcolleges maakt ook duidelijk op welk moment een indiener ermee bekend kan zijn dat de verstoring is verholpen.

Daarnaast kunnen er verstoringen zijn buiten het systeem waardoor er geen gebruik kan worden gemaakt van het systeem. Hierbij kan men denken aan stroomstoringen of storingen bij een provider van een partij. Ook dergelijke verstoringen zijn in beginsel niet toe te rekenen aan de partij die een stuk wil indienen. Het is dan aan de betrokken partij om te bewijzen dat een dergelijke verstoring heeft plaatsgevonden ter onderbouwing van de verschoonbaarheid van de termijnoverschrijding.

---

[10] Deze bepalingen zijn gebaseerd op vergelijkbare bepalingen in de artikelen 2:19 en 2:20 van de Algemene wet bestuursrecht. Zoals toegelicht op pagina 1 van deze nota van toelichting is de Awb niet van toepassing op het tuchtrecht voor de gezondheidszorg.

[11] Artikel 2:21 Algemene wet bestuursrecht.

Artikel II

Dit besluit bevat een gebruikelijke inwerkingtredingsbepaling op grond waarvan het tijdstip van inwerkingtreding bij koninklijk besluit wordt bepaald.

De Minister van Langdurige Zorg, Jeugd en Sport,