Richtsnoeren 4/2018 inzake de accreditatie van certificeringsorganen op grond van artikel 43 van de algemene verordening gegevensbescherming (2016/679)

Versie 3.0

4 juni 2019

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Vastgesteld

Versiegeschiedenis

Versie 3.0	4 juni 2019	Toevoeging van bijlage 1 (versie 2.0 van bijlage 1, vastgesteld op 4 juni 2019 na openbare raadpleging)
Versie 2.0	4 december 2018	Vaststelling van de richtsnoeren na openbare raadpleging — Op dezelfde datum werd bijlage 1 (versie 1.0) goedgekeurd voor openbare raadpleging.
Versie 1.0	6 februari 2018	Vaststelling van de richtsnoeren door de Groep gegevensbescherming artikel 29 (voor raadpleging bestemde versie). Deze versie werd op 25 mei 2018 door het Europees Comité voor gegevensbescherming bekrachtigd.

Inhoudsopgave

Het Europees Comité voor gegevensbescherming

Gezien artikel 70, lid 1, onder e), van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming),

Rekening houdend met de resultaten van de openbare raadpleging over de richtsnoeren, die in februari 2018 heeft plaatsgevonden, en die van de openbare raadpleging over de bijlage, die van 14 december 2018 tot 1 februari 2019 heeft plaatsgevonden, overeenkomstig artikel 70, lid 4, van de algemene verordening gegevensbescherming,

HEEFT DE VOLGENDE RICHTSNOEREN VASTGESTELD

1 INLEIDING

1. De algemene verordening gegevensbescherming (Verordening (EU) 2016/679), hierna "AVG" genoemd, die op 25 mei 2018 in werking is getreden, voorziet in een gemoderniseerd nalevingskader voor gegevensbescherming in Europa, dat gebaseerd is op het afleggen van rekenschap en op de grondrechten. In dit nieuwe kader staat een reeks maatregelen centraal ter facilitering van de naleving van de bepalingen van de AVG. Deze omvatten verplichtingen die in specifieke omstandigheden van kracht zijn (met inbegrip van de benoeming van functionarissen voor gegevensbescherming en het uitvoeren van gegevensbeschermingseffectbeoordelingen) en vrijwillige maatregelen zoals gedragscodes en certificeringsmechanismen.

2. In het kader van het vaststellen van certificeringsmechanismen en gegevensbeschermingszegels en -merktekens dienen lidstaten op grond van artikel 43, lid 1, AVG ervoor te zorgen dat certificeringsorganen die certificeringen verstrekken op grond van artikel 42, lid 1, AVG, worden geaccrediteerd door de bevoegde toezichthoudende autoriteit en/of de nationale accreditatie-instantie. Indien de accreditatie wordt uitgevoerd door de nationale accreditatie-instantie in overeenstemming met ISO/IEC 17065/2012, moeten tevens de door de bevoegde toezichthoudende autoriteit vastgestelde aanvullende eisen worden toegepast.

3. Nuttige certificeringsmechanismen kunnen zorgen voor betere naleving van de AVG en meer transparantie, zowel voor betrokkenen als in het kader van de betrekkingen tussen bedrijven onderling, bijvoorbeeld tussen verwerkingsverantwoordelijken en verwerkers. Voor verwerkingsverantwoordelijken en verwerkers is het nuttig te beschikken over een verklaring

van een onafhankelijke derde teneinde te kunnen aantonen dat hun verwerkingsactiviteiten voldoen aan de wettelijke vereisten[1].

4. In het kader hiervan erkent het Europees Comité voor gegevensbescherming (EDPB) dat het noodzakelijk is richtsnoeren te bieden ten aanzien van accreditatie. De specifieke waarde en het specifieke doel van accreditatie zijn gelegen in het feit dat daarmee een gezaghebbende verklaring van de bevoegdheid van certificeringsorganen wordt geboden, waardoor vertrouwen in het certificeringsmechanisme kan worden gewekt.

5. De richtsnoeren moeten dienen als leidraad voor de interpretatie en de uitvoering van artikel 43 AVG. In het bijzonder hebben zij tot doel om lidstaten, toezichthoudende autoriteiten en nationale accreditatie-instanties te ondersteunen bij het vaststellen van een consequent, geharmoniseerd referentiepunt voor de accreditatie van certificeringsorganen die tot taak hebben certificaten af te geven in overeenstemming met de AVG.

2 TOEPASSINGSGEBIED VAN DE RICHTSNOEREN

6. In deze richtsnoeren:

- wordt het doel van accreditatie in het kader van de AVG uiteengezet;
- worden de beschikbare trajecten voor de accreditatie van certificeringsorganen overeenkomstig artikel 43, lid 1, AVG toegelicht en worden de te overwegen belangrijkste aspecten aangegeven;
- wordt een kader geboden voor het vaststellen van aanvullende accreditatie-eisen wanneer de accreditatie wordt uitgevoerd door de nationale accreditatie-instantie, en
- wordt een kader geboden voor het vaststellen van accreditatie-eisen wanneer de accreditatie wordt uitgevoerd door de toezichthoudende autoriteit.

7. De richtsnoeren vormen geen procedurehandleiding voor de accreditatie van certificeringsorganen in overeenstemming met de AVG. Met de richtsnoeren wordt geen nieuwe technische norm voor de accreditatie van certificeringsorganen voor de toepassing van de AVG tot stand gebracht.

8. De richtsnoeren zijn bedoeld voor:

   - de lidstaten, die ervoor moeten zorgen dat certificeringsorganen worden geaccrediteerd door de toezichthoudende autoriteit en/of de nationale accreditatie-instantie;
   - de nationale accreditatie-instanties die de accreditatie van certificeringsorganen uitvoeren op grond van artikel 43, lid 1, onder b), AVG;
   - de bevoegde toezichthoudende autoriteit die “aanvullende eisen” op de eisen in ISO/IEC 17065/2012[2] formuleert, wanneer de accreditatie wordt uitgevoerd door de nationale accreditatie-instantie op grond van artikel 43, lid 1, onder b), AVG;

---

[1] In overweging 100 van de AVG wordt gesteld dat het instellen van certificeringsmechanismen de transparantie en naleving van de verordening kan versterken en betrokkenen in staat stelt het gegevensbeschermingsniveau van producten en diensten ter zake te beoordelen.

[2] Internationale organisatie voor standaardisatie: conformiteitsbeoordeling – Vereisten voor organen die producten, processen en diensten certificeren.

- het EDPB, bij het uitbrengen van adviezen inzake de accreditatie-eisen door bevoegde toezichthoudende autoriteiten en de goedkeuring van die eisen overeenkomstig artikel 43, lid 3, artikel 70, lid 1, onder p), en artikel 64, lid 1, onder c), AVG;
- de bevoegde toezichthoudende autoriteit, bij het vaststellen van de accreditatie-eisen wanneer de accreditatie wordt verricht door de toezichthoudende autoriteit overeenkomstig artikel 43, lid 1, onder a), AVG;
- overige belanghebbenden, zoals eventuele toekomstige certificeringsorganen of eigenaren van certificeringsregelingen die voorzien in certificeringscriteria en -procedures[3].

9. Definities

10. Het doel van de volgende definities is te zorgen voor een gemeenschappelijk begrip van de elementaire onderdelen van het accreditatieproces. Ze moeten worden gezien als referentiepunten maar dienen niet te worden opgevat als onbetwistbaar. Deze definities zijn gebaseerd op bestaande regelgevingskaders en -normen, met name ten aanzien van de relevante bepalingen van de AVG en ISO/IEC 17065/2012.

11. Voor de toepassing van deze richtsnoeren wordt verstaan onder:

12. "*accreditatie*" van certificeringsorganen: zie deel 3 over de interpretatie van accreditatie voor de toepassing van artikel 43 AVG;

13. "*aanvullende eisen*": de eisen die zijn vastgesteld door de bevoegde toezichthoudende autoriteit en op basis waarvan een accreditatie wordt uitgevoerd[4];

14. "*certificering*": het oordeel, en de attestatie van een onpartijdige derde[5], dat de vervulling van certificeringscriteria is aangetoond;

15. "*certificeringsorgaan*": een orgaan[6] voor conformiteitsbeoordeling[7] dat als derde partij certificeringsmechanismen[8] beheert;

---

[3] De eigenaar van een regeling is een identificeerbare organisatie die de certificeringscriteria en de vereisten aan de hand waarvan de conformiteit wordt beoordeeld, heeft opgesteld. De accreditatie betreft de organisatie die beoordelingen uitvoert (artikel 43, lid 4, AVG) aan de hand van de vereisten van de certificeringsregeling en de certificaten verstrekt (d.w.z. het certificeringsorgaan, ook wel conformiteitsbeoordelingsorgaan). De organisatie die de beoordelingen uitvoert, kan dezelfde organisatie zijn die ook het programma heeft ontwikkeld en eigenaar van de regeling is. Het kan echter zo zijn geregeld dat de ene organisatie de eigenaar van de regeling is, terwijl een of meer andere organisaties de beoordelingen uitvoeren.

[4] Artikel 43, leden 1, 3 en 6, AVG.

[5] Volgens ISO 17000 is attestatie (certificering) door een derde vereist voor alle aan conformiteitsbeoordeling onderworpen objecten (5.5), behalve voor conformiteitsbeoordelingsinstanties zelf, waarvoor accreditatie vereist is (5.6).

[6] Zie ISO 17000, punt 2.5: "body that performs conformity assessment services" (instantie die conformiteitsbeoordelingsdiensten uitvoert); ISO 17011: "body that performs conformity assessment services and that can be the object of accreditation" (instantie die conformiteitsbeoordelingsdiensten uitvoert en het voorwerp van accreditatie kan zijn); ISO 17065, punt 3.12.

[7] Activiteiten in het kader van conformiteitsbeoordeling door een derde worden verricht door een organisatie die onafhankelijk is van de persoon of organisatie die aan de conformiteitsbeoordeling wordt onderworpen en van de belangen van de gebruikers daarvan, zie ISO 17000, punt 2.4.

16. "*certificeringsregeling*": een certificeringssysteem dat verband houdt met specifieke producten, processen en diensten waarop dezelfde specifieke eisen, voorschriften en procedures van toepassing zijn[9];

17. "*criteria*" of "*certificeringscriteria*": de criteria aan de hand waarvan een certificering (conformiteitsbeoordeling) wordt uitgevoerd[10];

18. "*nationale accreditatie-instantie*": de enige instantie in een lidstaat die overeenkomstig Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad door die staat gemachtigd is accreditaties te verlenen[11].

3 INTERPRETATIE VAN "ACCREDITATIE" VOOR DE TOEPASSING VAN ARTIKEL 43 AVG

19. De AVG geeft geen definitie van "accreditatie". In artikel 2, lid 10, van Verordening (EG) 765/2008, waarin algemene eisen voor accreditaties worden vastgesteld, wordt accreditatie gedefinieerd als:

20. "een formele verklaring van een nationale accreditatie-instantie dat een conformiteitsbeoordelingsinstantie voldoet aan de eisen die zijn bepaald door geharmoniseerde normen en, indien van toepassing, aanvullende eisen, zoals die welke zijn opgenomen in de relevante sectorale regelingen, om een specifieke conformiteitsbeoordelingsactiviteit te verrichten".

21. Overeenkomstig ISO/IEC 17011

22. "doelt accreditatie op een door een derde afgegeven formele verklaring betreffende een conformiteitsbeoordelingsinstantie waaruit blijkt dat deze instantie bekwaam is om specifieke conformiteitsbeoordelingstaken te verrichten."

23. In artikel 43, lid 1, AVG wordt bepaald:

24. "Onverminderd de taken en bevoegdheden van de bevoegde toezichthoudende autoriteit uit hoofde van de artikelen 57 en 58, gaan certificeringsorganen die over passende deskundigheid met betrekking tot gegevensbescherming beschikken, in voorkomend geval na kennisgeving aan de toezichthoudende autoriteit met het oog op de uitoefening van haar bevoegdheden overeenkomstig artikel 58, lid 2, punt h), over tot afgifte en verlenging van het certificaat. De lidstaten zorgen ervoor dat die certificeringsorganen worden geaccrediteerd door één van de volgende instanties:

    (a) de toezichthoudende autoriteit die bevoegd is overeenkomstig artikel 55 of 56;
    (b) de nationale accreditatie-instantie die is aangewezen in overeenstemming met Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad, in overeenstemming met EN-ISO/IEC 17065/2012 en met de aanvullende eisen die door de overeenkomstig artikel 55 of 56 bevoegde toezichthoudende autoriteit zijn vastgesteld."

---

[8] Artikel 42, leden 1 en 5, AVG.
[9] Zie punt 3.9, in samenhang met bijlage B bij ISO 17065.
[10] Zie artikel 42, lid 5.
[11] Zie artikel 2, punt 11, van Verordening (EG) nr. 765/2008.

25. Ten aanzien van de AVG worden de accreditatie-eisen gebaseerd op:

- ISO/IEC 17065/2012 en de "aanvullende eisen" die zijn vastgesteld door de toezichthoudende autoriteit die bevoegd is op grond van artikel 43, lid 1, onder b), AVG, wanneer de accreditatie wordt uitgevoerd door de nationale accreditatie-instantie, en door de toezichthoudende autoriteit wanneer deze de accreditatie zelf uitvoert.

26. In beide gevallen moeten de geconsolideerde eisen de in artikel 43, lid 2, AVG vermelde eisen omvatten.

27. Het EDPB erkent dat het doel van accreditatie is om een gezaghebbende verklaring af te geven omtrent de bevoegdheid van een instantie om de certificering (conformiteitsbeoordelingen) uit te voeren[12]. Accreditatie betekent in het kader van de AVG het volgende:

28. een door een nationale accreditatie-instantie en/of een toezichthoudende autoriteit afgegeven formele verklaring[13] dat een certificeringsorgaan[14] gekwalificeerd is om certificeringen uit te voeren op grond van de artikelen 42 en 43 AVG, rekening houdend met ISO/IEC 17065/2012 en de door de toezichthoudende autoriteit en/of door het Comité vastgestelde aanvullende eisen.

4 ACCREDITATIE IN DE ZIN VAN ARTIKEL 43, LID 1, AVG

29. In artikel 43, lid 1, AVG wordt erkend dat er verschillende opties zijn voor de accreditatie van certificeringsorganen. Op grond van de AVG wordt van toezichthoudende autoriteiten en lidstaten verlangd dat zij het proces voor de accreditatie van certificeringsorganen vastleggen. In dit gedeelte worden de in artikel 43 AVG vermelde accreditatietrajecten uiteengezet.

4.1 Rol van de lidstaten

30. Op grond van artikel 43, lid 1, AVG moeten de lidstaten *ervoor zorgen* dat certificeringsorganen worden geaccrediteerd. Het staat elke lidstaat wel vrij om te bepalen wie er verantwoordelijk voor is om de beoordeling voor een eventuele accreditatie uit te voeren. Op grond van artikel 43, lid 1, AVG zijn er drie opties; de accreditatie wordt uitgevoerd:

(1) uitsluitend door de toezichthoudende autoriteit, op basis van door haarzelf vastgestelde eisen;
(2) uitsluitend door de nationale accreditatie-instantie overeenkomstig Verordening (EG) nr. 765/2008 en op basis van ISO/IEC 17065/2012 en de door de bevoegde toezichthoudende autoriteit vastgestelde aanvullende eisen; of
(3) door zowel de toezichthoudende autoriteit als de nationale accreditatie-instantie (en overeenkomstig alle onder punt 2 vermelde vereisten).

---

[12] Vgl. Verordening (EG) nr. 765/2008, overweging 15.
[13] Vgl. artikel 2, punt 10, van Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten.
[14] Vgl. de definitie van de term "accreditatie" in de zin van ISO 17011.

31. Het is aan de afzonderlijke lidstaten om te beslissen of de nationale accreditatie-instantie dan wel de toezichthoudende autoriteit of beide tezamen deze accreditatie-activiteiten uitvoeren. In elk geval dient de lidstaat echter te voorzien in passende middelen[15].

4.2 Wisselwerking met Verordening (EG) nr. 765/2008

32. Het EDPB merkt op dat nationale accreditatie-instantie in artikel 2, punt 11, van Verordening (EG) nr. 765/2008 wordt gedefinieerd als "de enige instantie in een lidstaat die door die staat gemachtigd is accreditaties te verlenen".

33. Artikel 2, lid 11, kan worden gezien als niet in overeenstemming met artikel 43, lid 1, AVG, waarin wordt bepaald dat accreditaties ook kunnen worden uitgevoerd door een andere instantie dan de nationale accreditatie-instantie van de lidstaat. Het EDPB is van mening dat de EU-wetgeving hiermee doelbewust heeft willen afwijken van het algemene beginsel dat accreditatie uitsluitend door de nationale accreditatie-instantie mag worden uitgevoerd, door toezichthoudende autoriteiten dezelfde bevoegdheid te geven ten aanzien van de accreditatie van certificeringsorganen. Om die reden vormt artikel 43, lid 1, AVG een lex specialis ten opzichte van artikel 2, punt 11, van Verordening 765/2008.

4.3 Rol van de nationale accreditatie-instantie

34. In artikel 43, lid 1, onder b), AVG wordt bepaald dat de nationale accreditatie-instantie de certificeringsorganen accrediteert overeenkomstig ISO/IEC 17065/2012 en de door de bevoegde toezichthoudende autoriteit vastgestelde aanvullende eisen.

35. Duidelijkheidshalve merkt het EDPB op dat de specifieke verwijzing naar "lid 1, punt b)" in artikel 43, lid 3, AVG impliceert dat "die eisen" verwijst naar de "aanvullende eisen" die door de bevoegde toezichthoudende autoriteit ingevolge artikel 43, lid 1, onder b), AVG zijn vastgesteld en de vereisten die in artikel 43, lid 2, AVG zijn uiteengezet.

36. Tijdens het accreditatieproces passen de nationale accreditatie-instanties de aanvullende eisen toe die de toezichthoudende autoriteiten dienen vast te stellen.

37. Een certificeringsorgaan dat reeds is geaccrediteerd op basis van ISO/IEC 17065/2012 voor andere certificeringsregelingen dan die welke betrekking hebben op de AVG en ook geaccrediteerd wil worden voor certificeringen die worden afgegeven in overeenstemming met de AVG, dient te voldoen aan de aanvullende eisen die door de toezichthoudende autoriteit zijn vastgesteld, indien de accreditatie door de nationale accreditatie-instantie wordt verricht. Indien de accreditatie voor certificering op grond van de AVG uitsluitend door de bevoegde toezichthoudende autoriteit wordt verricht, moet een om accreditatie verzoekend certificeringsorgaan voldoen aan de eisen die door de betreffende toezichthoudende autoriteit zijn vastgesteld.

4.4 Rol van de toezichthoudende autoriteit

38. Het EDPB merkt op dat in artikel 57, lid 1, onder q), AVG wordt bepaald dat de toezichthoudende autoriteit dient te zorgen voor de accreditatie van een certificeringsorgaan op grond van artikel 43 AVG, als een van de taken die de toezichthoudende autoriteit heeft overeenkomstig artikel 57 AVG, terwijl in artikel 58, lid 3, onder e), AVG wordt bepaald dat de toezichthoudende autoriteit de autorisatie- en adviesbevoegdheden heeft om certificeringsorganen te accrediteren overeenkomstig artikel

[15] Zie artikel 4, lid 9, van Verordening (EG) nr. 765/2008.

43. De formulering van artikel 43, lid 1, AVG biedt enige flexibiliteit en de functie van de accreditatie door de toezichthoudende autoriteit mag alleen worden opgevat als een taak indien dit van toepassing is. De wetgeving van de lidstaten kan worden aangewend om dit punt te verduidelijken. Desondanks is het certificeringsorgaan – tijdens het proces van accreditatie door een nationale accreditatie-instantie – op grond van artikel 43, lid 2, onder a), AVG verplicht om ten genoegen van de bevoegde toezichthoudende autoriteit zijn onafhankelijkheid en deskundigheid aan te tonen met betrekking tot het onderwerp van het door het certificeringsorgaan aangeboden certificeringsmechanisme[16].

39. Indien een lidstaat bepaalt dat de certificeringsorganen door de toezichthoudende autoriteit moeten worden geaccrediteerd, dient de toezichthoudende autoriteit accreditatie-eisen vast te stellen, die onder meer ook de in artikel 43, lid 2, AVG vermelde eisen omvatten. In vergelijking met de plichten in verband met de accreditatie van certificeringsorganen door nationale accreditatie-instanties is artikel 43 AVG minder sturend ten aanzien van de accreditatie-eisen wanneer de toezichthoudende autoriteit zelf de accreditatie uitvoert. Om bij te dragen tot een geharmoniseerde benadering van accreditatie dient ISO/IEC 17065 leidend te zijn voor de door de toezichthoudende autoriteit gehanteerde accreditatiecriteria en dienen deze te worden aangevuld met de aanvullende eisen die een toezichthoudende autoriteit vaststelt op grond van artikel 43, lid 1, onder b), AVG. Het EDPB merkt op dat artikel 43, lid 2, onder a) tot en met e), AVG de eisen van ISO 17065 weerspiegelt en specificeert, hetgeen de samenhang ten goede komt.

40. Indien een lidstaat bepaalt dat de certificeringsorganen door de nationale accreditatie-instanties moeten worden geaccrediteerd, dient de toezichthoudende autoriteit aanvullende eisen vast te stellen, als aanvulling op de in Verordening (EG) nr. 765/2008 bedoelde accreditatieconventies (de artikelen 3 tot en met 14 van die verordening hebben betrekking op de wijze waarop de accreditatie van conformiteitsbeoordelingsinstanties wordt georganiseerd en uitgevoerd) en de technische voorschriften waarin de door de certificeringsorganen gehanteerde methoden en procedures worden beschreven. In dit licht bezien, biedt Verordening (EG) nr. 765/2008 verdere sturing: artikel 2, lid 10, geeft een definitie van accreditatie en verwijst daarbij naar “geharmoniseerde normen” en “aanvullende eisen, zoals die welke zijn opgenomen in de relevante sectorale regelingen”. Hieruit volgt dat de door de toezichthoudende autoriteit vastgestelde aanvullende eisen specifieke eisen dienen te omvatten en gericht moeten zijn op vergemakkelijking van de beoordeling van onder andere de onafhankelijkheid en het niveau van deskundigheid van de certificeringsorganen op het gebied van gegevensbescherming, bijvoorbeeld wat betreft hun bekwaamheid om activiteiten in verband met de verwerking van persoonsgegevens door verwerkingsverantwoordelijken en verwerkers op grond van artikel 42, lid 1, te beoordelen en te certificeren. Hieronder valt tevens de noodzakelijke bevoegdheid voor sectorale regelingen alsmede ten aanzien van de bescherming van fundamentele rechten en vrijheden van natuurlijke personen en in het bijzonder hun recht op bescherming van persoonsgegevens[17]. De bijlage bij deze richtsnoeren kan dienen als nuttige informatiebron voor bevoegde toezichthoudende autoriteiten bij het vaststellen van de “aanvullende eisen” in overeenstemming met artikel 43, lid 1, onder b), en lid 3, AVG.

---

[16] In de aanvullende eisen die door de toezichthoudende autoriteit op grond van artikel 43, lid 1, onder b), AVG worden vastgesteld, dienen vereisten inzake onafhankelijkheid en deskundigheid te worden gespecificeerd. Zie tevens bijlage 1 bij de richtsnoeren.

[17] Artikel 1, lid 2, AVG.

41. In artikel 43, lid 6, AVG wordt bepaald: “De in lid 3 van dit artikel bedoelde voorschriften en de in artikel 42, lid 5, bedoelde criteria worden door de toezichthoudende autoriteit in een eenvoudig toegankelijke vorm openbaar gemaakt.” Derhalve moeten omwille van de transparantie alle door een toezichthoudende autoriteit goedgekeurde criteria en eisen worden gepubliceerd. Wat betreft de kwaliteit van en het vertrouwen in de certificeringsorganen is het wenselijk dat het publiek rechtstreeks toegang heeft tot alle eisen voor accreditatie.

4.5 Toezichthoudende autoriteit die als certificeringsorgaan optreedt

42. In artikel 42, lid 5, AVG wordt bepaald dat een toezichthoudende autoriteit certificaten mag afgeven, maar volgens de AVG hoeft zij niet te worden geaccrediteerd om te voldoen aan de in Verordening (EG) nr. 765/2008 bedoelde eisen. Het EDPB merkt op dat bij artikel 43, lid 1, onder a), AVG en meer specifiek bij artikel 58, lid 2, onder h), en lid 3, onder a), e) en f), AVG toezichthoudende autoriteiten de bevoegdheid wordt verleend om zowel accreditatie als certificering uit te voeren en tegelijkertijd ook advies te verstrekken en, indien van toepassing, certificeringen in te trekken of certificeringsorganen te gelasten geen certificeringen af te geven.

43. Er kunnen zich omstandigheden voordoen waarin het aangewezen of vereist is om de rollen en plichten op het gebied van accreditatie en certificering te scheiden, bijvoorbeeld indien er in een lidstaat een toezichthoudende autoriteit en andere certificeringsorganen naast elkaar bestaan en beide dezelfde typen certificeringen afgeven. Toezichthoudende autoriteiten dienen derhalve voldoende organisatorische maatregelen te treffen om de taken uit hoofde van de AVG te scheiden, teneinde zodoende certificeringsmechanismen te verankeren en te faciliteren en tegelijkertijd voorzorgsmaatregelen te treffen ter voorkoming van belangenverstrengeling die eventueel uit deze taken zou kunnen volgen. Daarnaast dienen lidstaten en toezichthoudende autoriteiten, bij het formuleren van nationale wetgeving en procedures in verband met accreditatie en certificering in overeenstemming met de AVG, rekening te houden met het geharmoniseerde Europese niveau.

4.6 Accreditatie-eisen

44. De bijlage bij deze richtsnoeren geeft aanwijzingen voor het in kaart brengen van de aanvullende accreditatie-eisen. In de bijlage wordt vermeld welke bepalingen van de AVG relevant zijn en worden suggesties gedaan voor eisen die toezichthoudende autoriteiten en nationale accreditatie-instanties dienen te overwegen om naleving van de AVG te waarborgen.

45. Zoals hierboven vastgesteld, geldt, wanneer certificeringsorganen worden geaccrediteerd door de nationale accreditatie-instantie op grond van Verordening (EG) nr. 765/2008, ISO/IEC 17065/2012 als relevante accreditatienorm, aangevuld met de aanvullende eisen die zijn vastgesteld door de toezichthoudende autoriteit. Artikel 43, lid 2, AVG geeft de algemene bepalingen weer van ISO/IEC 17065/2012 in het licht van de bescherming van de grondrechten in het kader van de AVG. Het kader in de bijlage maakt gebruik van artikel 43, lid 2, AVG en ISO/IEC 17065/2012 als grondslag voor de vaststelling van eisen met daarbij verdere criteria in verband met de beoordeling van de deskundigheid van de certificeringsorganen op het gebied van gegevensbescherming en hun vermogen om de rechten en vrijheden van natuurlijke personen ten aanzien van het verwerken van persoonsgegevens, zoals vastgelegd in de AVG, te eerbiedigen. Het EDPB merkt op dat het zich met name richt op het waarborgen van een voldoende deskundigheidsniveau van

certificeringsorganen op het gebied van gegevensbescherming zoals bedoeld in artikel 43, lid 1, AVG.

46. De door de toezichthoudende autoriteit vastgestelde aanvullende accreditatie-eisen zijn van toepassing op alle om accreditatie verzoekende certificeringsorganen. De accreditatie-instantie zal beoordelen of desbetreffend certificeringsorgaan bekwaam is om de certificeringsactiviteit uit te voeren in overeenstemming met de aanvullende eisen en gezien het onderwerp van certificering. Er zal worden gerefereerd aan specifieke certificeringssectoren of -gebieden waarvoor het certificeringsorgaan wordt geaccrediteerd.

47. Het EDBP merkt tevens op dat, naast de eisen in ISO/IEC 17065/2012, bijzondere deskundigheid op het gebied van gegevensbescherming ook vereist is indien andere – externe – organen, zoals laboratoria en auditors, onderdelen of componenten van certificeringsactiviteiten uitvoeren namens een geaccrediteerd certificeringsorgaan. In die gevallen is accreditatie van deze externe organen op grond van de AVG zelf niet mogelijk. Om de geschiktheid van deze organen voor hun activiteit namens de geaccrediteerde certificeringsorganen te waarborgen, is het echter nodig dat het geaccrediteerde certificeringsorgaan ervoor zorgt dat de deskundigheid inzake gegevensbescherming die voor het geaccrediteerde orgaan is vereist, ook bij het externe orgaan aanwezig en aantoonbaar is ten aanzien van de uitgevoerde activiteit.

48. Het kader voor het vaststellen van de aanvullende accreditatie-eisen, zoals opgenomen in de bijlage bij deze richtsnoeren, vormt geen procedurele handleiding voor het accreditatieproces zoals dit wordt uitgevoerd door de nationale accreditatie-instantie of de toezichthoudende autoriteit. Wel biedt het kader richtsnoeren ten aanzien van opzet en methodiek, en krijgen zodoende de toezichthoudende autoriteiten instrumenten aangereikt om de aanvullende accreditatie-eisen vast te stellen.

BIJLAGE 1

Bijlage 1 bevat richtsnoeren voor de formulering van "aanvullende" accreditatie-eisen met betrekking tot ISO/IEC 17065/2012 en overeenkomstig artikel 43, lid 1, onder b), en lid 3, AVG.

Deze bijlage bevat suggesties voor de eisen die een toezichthoudende autoriteit voor gegevensbescherming moet opstellen en die van toepassing zijn bij de accreditatie van een certificeringsorgaan door de nationale accreditatie-instantie of door de bevoegde toezichthoudende autoriteit[18]. Deze aanvullende eisen moeten overeenkomstig artikel 64, lid 1, onder c), AVG aan het Europees Comité voor gegevensbescherming worden meegedeeld alvorens te worden goedgekeurd.

Deze bijlage moet worden gelezen in samenhang met ISO/IEC 17065/2012. De hier gebruikte nummering komt overeen met die in ISO/IEC 17065/2012. Wanneer toezichthoudende autoriteiten overeenkomstig artikel 43, lid 1, onder a), AVG accreditatie verlenen, zou het een goede praktijk zijn deze aanpak waar mogelijk op te volgen. De geharmoniseerde accreditatie in de EU wordt hierdoor ondersteund.

Ongeacht de volgende richtsnoeren of het ontbreken van richtsnoeren betreffende een onderdeel van ISO/IEC 17065/2012, mag de bevoegde toezichthoudende autoriteit aanvullende eisen formuleren met betrekking tot deze onderdelen, indien zulks in overeenstemming is met de nationale wetgeving.

0 VOORBEPALING

[Dit onderdeel bevat eventuele overeengekomen samenwerkingsvoorwaarden tussen de nationale accreditatie-instantie en de toezichthoudende autoriteit voor gegevensbescherming, bijvoorbeeld betreffende de vraag wie verantwoordelijk moet zijn voor de ontvangst van aanvragen of de wijze van organisatie van de erkenning van goedgekeurde criteria in het kader van het accreditatieproces.]

1 TOEPASSINGSGEBIED[19]

Het toepassingsgebied van ISO/IEC 17065/2012 geldt in overeenstemming met de AVG. De richtsnoeren voor accreditatie en certificering bieden nadere informatie. Bij de beoordeling door de nationale accreditatie-instantie en de bevoegde toezichthoudende autoriteit in het kader van het accreditatieproces moet rekening worden gehouden met het toepassingsgebied van een certificeringsmechanisme (bijvoorbeeld bij de certificering van clouddiensten voor gegevensverwerking), met name ten aanzien van de criteria, de deskundigheid en de evaluatiemethodologie. Het brede toepassingsgebied van ISO/IEC 17065/2012, dat producten, processen en diensten bestrijkt, mag de vereisten van de AVG niet afzwakken of daarboven prevaleren; een governancemechanisme mag bijvoorbeeld niet het enige onderdeel van een certificeringsmechanisme zijn, aangezien de certificering ook de activiteiten in het kader van de verwerking van persoonsgegevens moet omvatten. Overeenkomstig artikel 42, lid 1, AVG is certificering uitsluitend van toepassing op de verwerkingsactiviteiten van verwerkingsverantwoordelijken en verwerkers.

---

[18] Informatie over de goedkeuringsprocedure voor de certificeringscriteria is opgenomen in deel 4 van de richtsnoeren voor certificering.

[19] De nummering verwijst naar ISO/IEC 17065/2012.

2 REFERENTIENORMEN

De AVG heeft voorrang boven ISO/IEC 17065/2012. Indien in de aanvullende eisen of door een certificeringsmechanisme wordt verwezen naar andere ISO-normen, moeten deze worden geïnterpreteerd in overeenstemming met de voorschriften van de AVG.

3 TERMEN EN DEFINITIES

In het kader van deze bijlage zijn de termen en definities van de richtsnoeren inzake accreditatie (WP 261) en certificering (EDPB 1/2018) van toepassing en hebben deze voorrang op de ISO-definities.

4 ALGEMENE ACCREDITATIE-EISEN

4.1 Juridische en contractuele aangelegenheden

4.1.1 Wettelijke aansprakelijkheid

Een certificeringsorgaan moet (te allen tijde) ten genoegen van de nationale accreditatie-instantie of de bevoegde toezichthoudende autoriteit kunnen aantonen dat het beschikt over geactualiseerde procedures die aantonen dat het handelt in overeenstemming met de in de accreditatievoorwaarden opgenomen wettelijke aansprakelijkheid, met inbegrip van de aanvullende eisen met betrekking tot de toepassing van Verordening (EU) 2016/679. Aangezien het certificeringsorgaan zelf verwerkingsverantwoordelijke/verwerker is, moet het kunnen aantonen dat het in het kader van de certificeringsprocedure beschikt over met Verordening (EU) 2016/679 strokende procedures en maatregelen die specifiek zijn bedoeld voor de controle en verwerking van de persoonsgegevens van de organisatie die cliënt is.

Voorafgaand aan de accreditatie kan de bevoegde toezichthoudende autoriteit beslissen verdere eisen en procedures te formuleren ter controle van de naleving van de AVG door het certificeringsorgaan.

4.1.2 Certificeringsovereenkomst

De minimumeisen voor een certificeringsovereenkomst worden aangevuld met de volgende punten:

Het certificeringsorgaan moet aantonen dat zijn certificeringsovereenkomsten, in aanvulling op ISO/IEC 17065/2012:

1. van de aanvrager verlangen dat deze te allen tijde voldoet aan de algemene certificeringsvoorschriften in de zin van punt 4.1.2.2, letter a), van ISO/IEC 17065/2012 en aan de criteria die zijn goedgekeurd door de bevoegde toezichthoudende autoriteit of het EDPB, overeenkomstig artikel 43, lid 2, onder b), en artikel 42, lid 5, AVG;
2. de aanvrager verplichten volledige transparantie te bieden aan de bevoegde toezichthoudende autoriteit met betrekking tot de certificeringsprocedure, ook wat betreft contractueel vertrouwelijke aangelegenheden die verband houden met de naleving van de gegevensbeschermingsregels overeenkomstig artikel 42, lid 7, en artikel 58, lid 1, onder c), AVG;
3. de verantwoordelijkheid van de aanvrager voor de naleving van Verordening (EU) 2016/679 niet beperken, en de taken en bevoegdheden van de toezichthoudende autoriteit die overeenkomstig artikel 42, lid 5, AVG bevoegd is, onverlet laten;

4. van de aanvrager verlangen dat hij het certificeringsorgaan overeenkomstig artikel 42, lid 6, AVG alle nodige informatie verstrekt en toegang verschaft tot zijn verwerkingsactiviteiten, voor zover noodzakelijk voor de uitvoering van de certificeringsprocedure;
5. van de aanvrager verlangen dat deze de toepasselijke termijnen en procedures in acht neemt. De certificeringsovereenkomst moet bepalen dat de termijnen en procedures die bijvoorbeeld voortvloeien uit het certificeringsprogramma of andere regelgeving, moeten worden nageleefd en in acht genomen;
6. met betrekking tot 4.1.2.2, letter c), nr. 1), van ISO/IEC 17065/2012 voorschriften bevatten inzake geldigheid, verlenging en intrekking overeenkomstig artikel 42, lid 7, en artikel 43, lid 4, AVG, inclusief passende termijnen voor herbeoordeling of herziening (regelmatigheid) als bedoeld in artikel 42, lid 7, AVG;
7. het certificeringsorgaan toestaan alle informatie openbaar te maken die nodig is voor het afgeven van het certificaat overeenkomstig artikel 42, lid 8 en artikel 43, lid 5, AVG;
8. voorschriften bevatten betreffende de nodige voorzorgsmaatregelen voor het onderzoek van klachten in de zin van punt 4.1.2.2, letter c), nr. 2), en overeenkomstig letter j) uitdrukkelijke verklaringen bevatten inzake de structuur en de procedures voor klachtenbeheer als bedoeld in artikel 43, lid 2, onder d), AVG;
9. naast de minimumvereisten bedoeld in punt 4.1.2.2 van ISO/IEC 17065/2012, indien de intrekking of opschorting van de accreditatie van het certificeringsorgaan gevolgen heeft voor de cliënt, bepalen dat in dat geval ook rekening moet worden gehouden met alle gevolgen voor diens klanten;
10. van de aanvrager verlangen dat hij het certificeringsorgaan op de hoogte stelt van significante veranderingen in zijn feitelijke of juridische situatie en met betrekking tot de producten, processen en diensten waarop de certificering betrekking heeft.

4.1.3 Gebruik van gegevensbeschermingszegels en -merktekens

De certificaten, zegels en merktekens mogen uitsluitend worden gebruikt in overeenstemming met de artikelen 42 en 43 AVG en de richtsnoeren inzake accreditatie en certificering.

4.2 Onpartijdigheidsmanagement

De accreditatie-instantie ziet erop toe dat, naast het bepaalde in punt 4.2 van ISO/IEC 17065/2012:

1. het certificeringsorgaan voldoet aan de aanvullende eisen die de bevoegde toezichthoudende autoriteit heeft vastgesteld (krachtens artikel 43, lid 1, onder b), AVG):
    a. dat het certificeringsorgaan overeenkomstig artikel 43, lid 2, onder a), AVG separaat zijn onafhankelijkheid aantoont. Dit betekent in het bijzonder dat bewijs moet worden geleverd over de financiering van het certificeringsorgaan, voor zover die van invloed is op de verzekering van onpartijdigheid;
    b. dat zijn taken en verplichtingen niet leiden tot een belangenconflict als bedoeld in artikel 43, lid 2, onder e), AVG;
2. het certificeringsorgaan geen relevante banden heeft met de klant die door het orgaan wordt beoordeeld.

4.3 Aansprakelijkheid en financiering

Naast de eis in punt 4.3.1 van ISO/IEC 17065/2012 waarborgt de accreditatie-instantie op regelmatige basis dat het certificeringsorgaan passende maatregelen (zoals verzekeringen of reserves) heeft getroffen om aan zijn verplichtingen te voldoen in de geografische regio's waar het orgaan actief is.

4.4 Niet-discriminerende voorwaarden

De toezichthoudende autoriteit kan aanvullende eisen formuleren indien die in overeenstemming zijn met de nationale wetgeving.

4.5 Vertrouwelijkheid

De toezichthoudende autoriteit kan aanvullende eisen formuleren indien die in overeenstemming zijn met de nationale wetgeving.

4.6 Openbaar beschikbare informatie

Naast de eis in punt 4.6 van ISO/IEC 17065/2012 schrijft de accreditatie-instantie voor dat het certificeringsorgaan ten minste:

1. alle (actuele en eerdere) versies van de goedgekeurde criteria als bedoeld in artikel 42, lid 5, AVG en alle certificeringsprocedures bekendmaakt en gemakkelijk voor het publiek beschikbaar maakt, en daarbij in het algemeen de geldigheidsduur van het betrokken document vermeldt;
2. informatie over klachtenprocedures en beroepsprocedures bekendmaakt overeenkomstig artikel 43, lid 2, onder d), AVG.

5 STRUCTURELE EISEN (ARTIKEL 43, LID 4, AVG ["JUISTE BEOORDELING"])

5.1 Organisatiestructuur en topmanagement

De toezichthoudende autoriteit kan aanvullende eisen formuleren.

5.2 Mechanismen ter waarborging van onpartijdigheid

De toezichthoudende autoriteit kan aanvullende eisen formuleren.

6 BENODIGDE MIDDELEN

6.1 Personeel van het certificeringsorgaan

Naast de eis in punt 6 van ISO/IEC 17065/2012 zorgt de accreditatie-instantie ervoor dat het personeel van ieder certificeringsorgaan:

1. aantoonbaar over passende en actuele deskundigheid (kennis en ervaring) beschikt op het gebied van gegevensbescherming, overeenkomstig artikel 43, lid 1, AVG;
2. onafhankelijk is en deskundig is ten aanzien van het te certificeren object, overeenkomstig artikel 43, lid 2, onder a), en dat er geen sprake is van een belangenconflict, overeenkomstig artikel 43, lid 2, onder e);
3. zich ertoe verbindt de in artikel 42, lid 5, AVG bedoelde criteria te eerbiedigen, overeenkomstig artikel 43, lid 2, onder b);

4. beschikt over relevante en passende kennis van en ervaring met de toepassing van de wetgeving inzake gegevensbescherming;
5. beschikt over relevante en passende kennis van en ervaring met de relevante technische en organisatorische maatregelen op het gebied van gegevensbescherming;
6. aantoonbare ervaring heeft op de gebieden vermeld in de aanvullende eisen, meer bepaald die genoemd in de punten 6.1.1, 6.1.4 en 6.1.5.

Voor personeel met technische expertise is vereist:

- Een kwalificatie op een relevant gebied van technische deskundigheid op ten minste EQF[20]-niveau 6, of een erkende beschermde titel (bv. Dipl. Ing.) voor het betrokken gereglementeerde beroep, dan wel significante beroepservaring.
- *Personeelsleden die verantwoordelijk zijn voor certificeringsbesluiten* moeten aanzienlijke beroepservaring hebben op het gebied van het vaststellen en uitvoeren van gegevensbeschermingsmaatregelen.
- *Personeelsleden die verantwoordelijk zijn voor evaluaties* moeten beroepservaring hebben op het gebied van technische gegevensbescherming, alsmede kennis en ervaring met een vergelijkbare procedure (bv. certificering of audit) en als zodanig zijn geregistreerd.

De personeelsleden moeten kunnen aantonen dat zij hun domeinspecifieke kennis op het gebied van technische en auditvaardigheden bijhouden door middel van continue professionele ontwikkeling.

Voor personeel met juridische expertise:

- Een rechtenstudie aan een door de EU of de staat erkende universiteit met een duur van ten minste acht semesters, die opleidt tot de academische graad master (LL.M.) of equivalent, dan wel aanzienlijke beroepservaring.
- *Personeelsleden die verantwoordelijk zijn voor de certificeringsbesluiten* moeten aanzienlijke beroepservaring aantonen op het gebied van gegevensbescherming en volgens de in hun lidstaat geldende regels geregistreerd zijn.
- *Personeelsleden die verantwoordelijk zijn voor evaluaties* moeten ten minste twee jaar beroepservaring hebben op het gebied van gegevensbescherming en kennis en ervaring met vergelijkbare procedures (bv. certificeringen/audits) en geregistreerd zijn door de lidstaat, indien dat vereist is.
    - De personeelsleden moeten kunnen aantonen dat zij hun domeinspecifieke kennis op het gebied van technische en auditvaardigheden bijhouden door middel van continue professionele ontwikkeling.

6.2 Middelen voor evaluatie

De toezichthoudende autoriteit kan aanvullende eisen formuleren indien die in overeenstemming zijn met de nationale wetgeving.

7 PROCESVEREISTEN (ARTIKEL 43, LID 2, ONDER C) EN D), AVG)

7.1 Algemeen

Naast de eis in punt 7.1 van ISO/IEC 17065/2012 moet de accreditatie-instantie worden verplicht:

1. ervoor zorgen dat de certificeringsorganen bij de indiening van de aanvraag voldoen aan de aanvullende eisen die door de bevoegde toezichthoudende autoriteit zijn vastgesteld

[20] Zie de vergelijkingstool van het kwalificatiekader op https://ec.europa.eu/ploteus/en/compare

(krachtens artikel 43, lid 1, onder b), AVG), zodat taken en verplichtingen niet leiden tot een belangenconflict als bedoeld in artikel 43, lid 2, onder b);

2. de relevante bevoegde toezichthoudende autoriteiten inlichten voordat een certificeringsorgaan vanuit een bijkantoor begint te werken met een goedgekeurd Europees gegevensbeschermingszegel in een nieuwe lidstaat.

7.2 Aanvraag

In aanvulling op punt 7.2 van ISO/IEC 17065/2012 dient de eis te gelden dat:

1. het te certificeren object (Target of Evaluation, ToE) in de aanvraag uitvoerig wordt beschreven. Daaronder vallen ook interfaces en overdrachten naar andere systemen en organisaties, protocollen en andere zekerheden;
2. in de aanvraag wordt vermeld of verwerkers worden ingezet; wanneer de aanvrager een verwerker is, moeten diens verantwoordelijkheden en taken worden beschreven en moeten de relevante overeenkomst(en) tussen de verwerkingsverantwoordelijke en de verwerker bij de aanvraag worden toegevoegd.

7.3 Toetsing van de aanvraag

In aanvulling op punt 7.3 van ISO/IEC 17065/2012 dient de eis te gelden dat:

1. in de certificeringsovereenkomst bindende evaluatiemethoden met betrekking tot het Target of Evaluation (ToE) zijn vastgesteld;
2. bij de beoordeling (punt 7.3, onder e)) van de vraag of de deskundigheid toereikend is, in passende mate rekening wordt gehouden met zowel technische als juridische deskundigheid op het gebied van gegevensbescherming.

7.4 Evaluatie

Naast het in punt 7.4 van ISO/IEC 17065/2012 bepaalde moeten in de certificeringsmechanismen evaluatiemethoden worden beschreven die toereikend zijn om te beoordelen of de verwerkingsactiviteiten voldoen aan de certificeringscriteria, met inbegrip van bijvoorbeeld:

1. een methode voor het beoordelen van de noodzaak en de evenredigheid van de verwerkingen, wat het doel en de betrokkenen betreft;
2. een methode voor het beoordelen van de dekking, samenstelling en beoordeling van alle risico's die door de verwerkingsverantwoordelijke en de verwerker in overweging worden genomen wat hun juridische consequenties betreft, overeenkomstig de artikelen 30, 32, 35 en 36 AVG, en wat de definitie van technische en organisatorische maatregelen betreft, overeenkomstig de artikelen 24, 25 en 32 AVG, voor zover de genoemde artikelen van toepassing zijn op het te certificeren object, en
3. een methode voor het beoordelen van de corrigerende maatregelen, waaronder garanties, waarborgen en procedures, die de bescherming verzekeren van de persoonsgegevens die zullen worden verwerkt door het te certificeren object, en voor het aantonen dat aan de wettelijke voorschriften van de criteria is voldaan; en
4. documentatie over de toegepaste methoden en bevindingen.

Het certificeringsorgaan moet worden verplicht ervoor te zorgen dat de evaluatiemethoden gestandaardiseerd en algemeen toepasbaar zijn. Dit betekent dat voor vergelijkbare Targets of Evaluation vergelijkbare evaluatiemethoden worden toegepast. Elke afwijking van deze procedure moet door het certificeringsorgaan worden gemotiveerd.

In aanvulling op punt 7.4.2 van ISO/IEC 17065/2012 moet worden toegestaan dat de evaluatie wordt uitgevoerd door externe deskundigen die door het certificeringsorgaan zijn erkend.

In aanvulling op punt 7.4.5 van ISO/IEC 17065/2012 moet de eis gelden dat gegevensbeschermingscertificering overeenkomstig de artikelen 42 en 43 AVG, waarbij het te certificeren object reeds deels is gecertificeerd, in een nieuwe certificering in aanmerking kan worden genomen. Het zal echter niet volstaan om (gedeeltelijke) evaluaties volledig te vervangen. Het certificeringsorgaan moet nagaan of aan de criteria wordt voldaan. Voor erkenning dient in ieder geval een volledig evaluatieverslag, of informatie die een evaluatie van de eerdere certificeringsactiviteit en de resultaten daarvan mogelijk maakt, beschikbaar te zijn. Een certificeringsverklaring of een soortgelijk certificaat mag niet als voldoende gelden om een verslag te vervangen.

In aanvulling op punt 7.4.6 van ISO/IEC 17065/2012 moet worden verlangd dat het certificeringsorgaan in zijn certificeringsmechanisme in detail beschrijft hoe de klant (certificatieaanvrager) door middel van de onder punt 7.4.6 gevraagde informatie wordt ingelicht over onregelmatigheden waarvan een certificeringsmechanisme blijk geeft. In dit verband moeten ten minste de aard en de timing van dergelijke informatie worden gedefinieerd.

In aanvulling op punt 7.4.9 van ISO/IEC 17065/2012 moet de eis gelden dat de documentatie desgevraagd volledig toegankelijk wordt gemaakt voor de toezichthoudende autoriteit voor gegevensbescherming.

7.5 Toetsing

Naast punt 7.5 van ISO/IEC 17065/2012 zijn procedures vereist voor de verlening, regelmatige herziening en intrekking van de certificaten die zijn afgegeven overeenkomstig artikel 43, lid 2 respectievelijk lid 3.

7.6 Certificeringsbesluit

In aanvulling op punt 7.6.1 van ISO/IEC 17065/2012 moet het certificeringsorgaan in zijn procedures gedetailleerd beschrijven hoe de onafhankelijkheid en de verantwoordelijkheid van het certificeringsorgaan met betrekking tot de individuele certificeringsbesluiten zijn gewaarborgd.

7.7 Documentatie inzake certificering

Naast punt 7.7.1.e van ISO/IEC 17065/2012 en overeenkomstig artikel 42, lid 7, AVG dient te worden bepaald dat de geldigheidsduur van certificaten niet langer mag zijn dan drie jaar.

Naast punt 7.7.1.e van ISO/IEC 17065/2012 moet de verplichting gelden dat de periode van geplande monitoring als bedoeld in punt 7.9 ook wordt gedocumenteerd.

Naast punt 7.7.1.f van ISO/IEC 17065/2012 moet het certificeringsorgaan worden verplicht het te certificeren object te vermelden in de certificeringsdocumenten (in voorkomend geval onder vermelding van de status van de desbetreffende versie of een soortgelijk kenmerk).

7.8 Lijst van gecertificeerde producten

Naast punt 7.8 van ISO/IEC 17065/2012 moet het certificeringsorgaan worden verplicht de informatie over gecertificeerde producten, processen en diensten intern en openbaar beschikbaar te stellen. Het certificeringsorgaan verstrekt het publiek een samenvatting van het evaluatieverslag. Het doel van deze samenvatting is transparantie te bevorderen met betrekking tot het gecertificeerde object en hoe dit is beoordeeld. In de samenvatting wordt uitleg gegeven over zaken als:

(a) de reikwijdte van de certificering en een zinvolle beschrijving van het te certificeren object (ToE);

(b) de respectieve certificeringscriteria (met inbegrip van de versie of de functionele status);

(c) de toegepaste evaluatiemethoden en tests, en

(d) het resultaat of de resultaten.

In aanvulling op punt 7.8 van ISO/IEC 17065/2012 en overeenkomstig artikel 43, lid 5, AVG stelt het certificeringsorgaan de bevoegde toezichthoudende autoriteiten in kennis van de redenen voor het verlenen of intrekken van de gevraagde certificering.

7.9 Toezicht

Naast de punten 7.9.1, 7.9.2 en 7.9.3 van ISO/IEC 17065/2012 en artikel 43, lid 2, onder c), AVG moet de verplichting gelden maatregelen voor regelmatige monitoring te nemen om ervoor te zorgen dat de certificering gedurende de monitoringperiode kan worden gehandhaafd.

7.10 Wijzigingen die van invloed zijn op de certificering

Naast het in de punten 7.10.1 en 7.10.2 van EN ISO/IEC 17065/2012 vermelde, moet onder meer het onderstaande worden beschouwd als wijzigingen die van invloed zijn op de certificering en door het certificeringsorgaan moeten worden beoordeeld: wijzigingen van de wetgeving inzake gegevensbescherming, de vaststelling van gedelegeerde handelingen van de Europese Commissie overeenkomstig artikel 43, leden 8 en 9, AVG, besluiten van het Europees Comité voor gegevensbescherming en rechterlijke beslissingen in verband met gegevensbescherming. De wijzigingsprocedures die hier worden overeengekomen, zouden onder meer het volgende kunnen omvatten: overgangsperioden, goedkeuringsprocessen voor de bevoegde toezichthoudende autoriteit, herbeoordeling van het relevante te certificeren object en passende maatregelen om de certificering in te trekken als de gecertificeerde verwerking niet langer aan de geactualiseerde criteria voldoet.

7.11 Beëindiging, vermindering, schorsing of intrekking van certificering

Naast hoofdstuk 7.11.1 van ISO/IEC 17065/2012 moet het certificeringsorgaan worden verplicht de bevoegde toezichthoudende autoriteit en de nationale accreditatie-instantie zo nodig schriftelijk in kennis te stellen van de genomen maatregelen en van de handhaving, beperking, opschorting en intrekking van de certificering.

Overeenkomstig artikel 58, lid 2, onder h), AVG is het certificeringsorgaan verplicht besluiten en bevelen van de bevoegde toezichthoudende autoriteit om de certificering van een cliënt (aanvrager) in te trekken of niet af te geven indien niet of niet meer aan de certificeringseis wordt voldaan, te aanvaarden.

7.12 Opgeslagen gegevens

Het certificeringsorgaan moet worden verplicht ervoor te zorgen dat alle documentatie volledig, begrijpelijk, actueel en voor audit blijft.

7.13 Klachten en beroepen (artikel 43, lid 2, onder d), AVG)

In aanvulling op punt 7.13.1 van ISO/IEC 17065/2012 moet het certificeringsorgaan vaststellen:

(a) wie klachten of bezwaren kan indienen;

(b) wie deze namens het certificeringsorgaan verwerkt;

(c) welke verificaties in dit verband plaatsvinden; en

(d) welke mogelijkheden er zijn voor het raadplegen van belanghebbenden.

In aanvulling op punt 7.13.1 van ISO/IEC 17065/2012 moet het certificeringsorgaan vaststellen:

(a) op welke wijze en aan wie de desbetreffende bevestiging moet worden gegeven,

(b) de daarvoor geldende termijnen; en

(c) welke processen vervolgens moeten worden gestart.

Naast punt 7.13.1 van ISO/IEC 17065/2012 moet het certificeringsorgaan bepalen hoe de scheiding tussen certificeringsactiviteiten en de behandeling van beroepen en klachten wordt gewaarborgd.

8 EISEN MET BETREKKING TOT HET MANAGEMENTSYSTEEM

Een algemene eis van het managementsysteem overeenkomstig hoofdstuk 8 van ISO/IEC 17065/2012 is dat de uitvoering door de geaccrediteerde certificatie-instantie van alle voorschriften van de voorgaande hoofdstukken binnen het toepassingsgebied van het certificeringsmechanisme onafhankelijk wordt gedocumenteerd, geëvalueerd, gecontroleerd en gemonitord.

Het basisbeginsel van het management is dat een systeem wordt gedefinieerd aan de hand waarvan, door middel van passende specificaties, op doeltreffende en efficiënte wijze doelen worden gesteld, en met name de uitvoering van de certificatiediensten. Dit vereist transparantie en controleerbaarheid van de uitvoering van de accreditatievereisten door het certificeringsorgaan en de permanente naleving ervan.

Daartoe moet in het managementsysteem een methode worden vastgesteld om deze eisen te vervullen en te controleren overeenkomstig de voorschriften inzake gegevensbescherming en deze voortdurend te controleren bij de geaccrediteerde instantie zelf.

Deze managementbeginselen en de gedocumenteerde tenuitvoerlegging ervan moeten transparant zijn en moeten door het geaccrediteerde certificeringsorgaan worden bekendgemaakt tijdens de accreditatieprocedure overeenkomstig artikel 58 AVG en daarna te allen tijde, op verzoek van de toezichthoudende autoriteit voor gegevensbescherming, wanneer een onderzoek plaatsvindt in de vorm van gegevensbeschermingscontroles als bedoeld in artikel 58, lid 1, onder b), AVG of een toetsing van de overeenkomstig artikel 42, lid 7, AVG afgegeven certificeringen als bedoeld in artikel 58, lid 1, onder c), AVG.

Met name dient het geaccrediteerde certificeringsorgaan te allen tijde openbaar te maken welke certificeringen die zijn uitgevoerd en op basis waarvan (of volgens welke certificeringsmechanismen of -regelingen), hoe lang de certificering geldig is, in welk kader en onder welke voorwaarden (overweging 100).

8.1 Algemene vereisten met betrekking tot het managementsysteem

De bevoegde toezichthoudende autoriteit kan verdere aanvullende eisen vaststellen en toevoegen indien dit in overeenstemming is met de nationale wetgeving.

8.2 Documentatie van het managementsysteem

De bevoegde toezichthoudende autoriteit kan verdere aanvullende eisen vaststellen en toevoegen indien dit in overeenstemming is met de nationale wetgeving.

8.3 Documentenbeheer

De bevoegde toezichthoudende autoriteit kan verdere aanvullende eisen vaststellen en toevoegen indien dit in overeenstemming is met de nationale wetgeving.

8.4 Beheer van registers

De bevoegde toezichthoudende autoriteit kan verdere aanvullende eisen vaststellen en toevoegen indien dit in overeenstemming is met de nationale wetgeving.

8.5 Managementtoetsing

De bevoegde toezichthoudende autoriteit kan verdere aanvullende eisen vaststellen en toevoegen indien dit in overeenstemming is met de nationale wetgeving.

8.6 Interne audits

De bevoegde toezichthoudende autoriteit kan verdere aanvullende eisen vaststellen en toevoegen indien dit in overeenstemming is met de nationale wetgeving.

8.7 Corrigerende maatregelen

De bevoegde toezichthoudende autoriteit kan verdere aanvullende eisen vaststellen en toevoegen indien dit in overeenstemming is met de nationale wetgeving.

8.8 Preventieve maatregelen

De bevoegde toezichthoudende autoriteit kan verdere aanvullende eisen vaststellen en toevoegen indien dit in overeenstemming is met de nationale wetgeving.

9 VERDERE AANVULLENDE EISEN[21]

9.1 Actualisering van de evaluatiemethoden

De certificerende instantie dient procedures vast te stellen voor het actualiseren van de evaluatiemethoden die in het kader van de in punt 7.4 bedoelde evaluatie worden toegepast. Actualisering moet plaatsvinden bij verandering van het rechtskader, de relevante risico's, de stand van de techniek en de uitvoeringskosten van de technische en organisatorische maatregelen.

9.2 Behoud van deskundigheid

De certificeringsorganen moeten procedures vaststellen met het oog op de opleiding van hun werknemers om hun vaardigheden te actualiseren, rekening houdend met de in punt 9.1 genoemde ontwikkelingen.

9.3 Verantwoordelijkheden en competenties

9.3.1 Communicatie tussen het certificeringsorgaan en zijn cliënten

Er dienen procedures te bestaan voor de uitvoering van passende procedures en structuren voor de communicatie tussen het certificeringsorgaan en zijn klant. Dit houdt in:

1. het bijhouden van documentatie betreffende de taken en verantwoordelijkheden door het geaccrediteerde certificeringsorgaan in verband met:
    a. verzoeken om informatie; of
    b. het opnemen van contact bij een klacht over certificering.

[21] De bevoegde toezichthoudende autoriteit kan verdere aanvullende eisen vaststellen en toevoegen indien dit in overeenstemming is met de nationale wetgeving.

2. het beschikken over een aanvraagprocedure voor
    a. informatie over de status van een aanvraag;
    b. evaluaties door de bevoegde toezichthoudende autoriteit met betrekking tot
        i. feedback;
        ii. besluiten van de bevoegde toezichthoudende autoriteit.

9.3.2 Documentatie van de evaluatieactiviteiten

De toezichthoudende autoriteit kan aanvullende eisen formuleren.

9.3.3 Beheer van de behandeling van klachten

Er moet een systeem voor klachtenbehandeling worden opgezet dat een integrerend onderdeel uitmaakt van het managementsysteem, dat met name moet voldoen aan de voorschriften van punt 4.1.2.2, letters c) en j), punt 4.6, letter d), en punt 7.13 van ISO/IEC 17065/2012.

Relevante klachten en bezwaren dienen te worden gedeeld met de bevoegde toezichthoudende autoriteit.

9.3.4 Management van de intrekking van accreditatie

De procedures in geval van schorsing of intrekking van de accreditatie worden geïntegreerd in het beheersysteem van het certificeringsorgaan, met inbegrip van de kennisgevingen aan klanten.