STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 30081
16 juni 2021

NL aanvullende accreditatie-eisen voor certificeringsorganen[1], Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens (hierna: AP) heeft op 8 juni 2021 het volgende besluit genomen inzake de aanvullende accreditatie-eisen voor certificeringsorganen met betrekking tot ISO/IEC 17065:2012 (hierna: ISO 17065) en overeenkomstig artikel 43, eerste lid, onder b, en artikel 43, derde lid, van de AVG:

De onderstaande punten (afgezien van punt 9) verwijzen naar de secties in ISO 17065 en geven de aanvullende eisen weer voor de desbetreffende ISO 17065-normelementen.

0 Voorwoord

De taken en verantwoordelijkheden van de AP en de Raad voor Accreditatie (hierna: RvA) als de nationale accreditatie-instantie (NAI) met betrekking tot accreditatie voor AVG-certificeringsschema's zijn beschreven in de *Uitvoeringswet Algemene Verordening Gegevensbescherming* (hierna: UAVG) en in een ministeriële regeling (*Regeling van de Minister voor Rechtsbescherming van 16 mei 2018 tot aanwijzing van de Raad voor Accreditatie als accrediterende instantie als bedoeld in artikel 43, eerste lid, van de Algemene verordening gegevensbescherming*).[2] De operationele procedures met betrekking tot de accreditatie voor AVG-certificeringsschema's zijn vastgelegd in een informatieprotocol tussen de AP en de RvA.[3]

1 Reikwijdte

Dit document bevat aanvullende eisen bij ISO 17065 voor de beoordeling van de competentie, de consistente werkwijze en de onpartijdigheid van AVG-certificeringsorganen.

De reikwijdte van ISO 17065 wordt toegepast in overeenstemming met de AVG. In de EDPB-richtsnoeren inzake accreditatie en certificering wordt nadere informatie gegeven. De brede reikwijdte van ISO 17065, die producten, processen en diensten omvat, prevaleert niet boven de AVG of doet hier geen afbreuk aan. Derhalve moet certificering betrekking hebben op de verwerking van persoonsgegevens. En hoewel een governancesysteem, bijvoorbeeld een privacy-informatiemanagementsysteem, deel kan uitmaken van een certificeringsmechanisme, mag het niet het enige element zijn.

De reikwijdte van een certificeringsmechanisme, bijvoorbeeld de certificering van de verwerking van clouddiensten, moet worden meegenomen in de beoordeling door de RvA en de AP tijdens het accreditatieproces, met name ten aanzien van criteria, deskundigheid en evaluatiemethodiek.

Ten slotte kan op grond van artikel 42, eerste lid, van de AVG alleen een AVG-certificering worden toegekend met betrekking tot de verwerkingsactiviteiten van de verwerkingsverantwoordelijke en de verwerker.

2 Normatieve referentie

De AVG prevaleert boven ISO 17065. Indien in de aanvullende eisen of door middel van een certificeringsmechanisme wordt verwezen naar andere ISO-normen, worden deze geïnterpreteerd in overeenstemming met de eisen die in de AVG zijn vastgesteld.

3 Termen en begripsomschrijvingen

De termen en begripsomschrijvingen van de richtsnoeren inzake accreditatie[4] en certificering[5] zijn van toepassing en hebben voorrang op de ISO-definities. Voor het gemak worden de belangrijkste definities die in dit document worden gebruikt, hieronder opgesomd.
• *Algemene verordening gegevensbescherming (AVG):* Verordening (EU) 2016/679.

---

1 De tekst van deze aanvullende eisen in de Engelse taal is authentiek. Bij interpretatieverschillen is de Engelse tekst leidend.
2 Staatscourant 2018, 28116.
3 Staatscourant 2020, 11507.
4 Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation.
5 Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation.

• *UAVG: Uitvoeringswet Algemene Verordening Gegevensbescherming*, de Nederlandse wet voor uitvoering van de AVG.
• *ISO 17065:* ISO/IEC 17065:2012.
• *Certificering:* de beoordeling en het onpartijdige attest van een derde partij dat de naleving van de certificeringscriteria is aangetoond met betrekking tot de verwerkingsactiviteiten van een verwerkingsverantwoordelijke of een verwerker.
• *Accreditatie:* attest van een derde partij met betrekking tot de activiteiten van een certificeringsorgaan. Dit is het resultaat van het beoordelingsproces voor een succesvol certificeringsorgaan (als onderdeel van het accreditatieproces).
• *Nationale accreditatie-instantie (NAI):* de enige instantie in een lidstaat die door die staat gemachtigd is accreditaties te verlenen overeenkomstig Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad. In Nederland is de Raad voor Accreditatie (RvA) de NAI.
• *Accreditatie-instantie:* instantie die de accreditatie uitvoert. In dit document wordt met deze term de RvA bedoeld.
• *Certificeringsorgaan:* derde-partij-conformiteitsbeoordelingsinstantie die certificeringsschema's uitvoert.
• *Certificeringscriteria:* de criteria waaraan de verwerkingsactiviteiten van een organisatie worden getoetst voor een bepaald certificeringsschema.
• *Certificeringsschema:* een certificeringssysteem met betrekking tot gespecificeerde producten, processen en diensten waarop dezelfde gespecificeerde eisen, specifieke regels en procedures van toepassing zijn. Het omvat de certificeringscriteria en de beoordelingsmethodologie.
• *Certificeringsmechanisme:* een goedgekeurd certificeringsschema dat beschikbaar is voor de aanvrager. Het is een dienst die wordt verleend door een geaccrediteerd certificeringsorgaan op basis van goedgekeurde criteria en beoordelingsmethodologie. Het is het systeem waarmee een verwerkingsverantwoordelijke of een verwerker wordt gecertificeerd.
• *Target of Evaluation (ToE):* het voorwerp van de certificering. In het geval van een AVG-certificering zijn dit de relevante verwerkingen die de verwerkingsverantwoordelijke of verwerker aanvraagt ter evaluatie en certificering.
• *Aanvrager:* de organisatie die een aanvraag heeft ingediend om haar verwerkingsactiviteiten te laten certificeren.
• *Cliënt:* de organisatie die is gecertificeerd (voorheen de aanvrager).

4 Algemene eisen voor accreditatie

4.1 Juridische en contractuele aangelegenheden

4.1.1 Wettelijke verantwoordelijkheid

Een certificeringsorgaan moet (te allen tijde) aan de RvA kunnen aantonen te beschikken over up-to-date procedures waaruit blijkt dat de wettelijke verantwoordelijkheden worden nageleefd die zijn vastgelegd in de accreditatievoorwaarden, inclusief de aanvullende eisen met betrekking tot de toepassing van de AVG.

Het certificeringsorgaan dient aan te kunnen tonen dat zijn procedures en maatregelen die specifiek gericht zijn op de controle en behandeling van de persoonsgegevens van de organisatie van de aanvrager en de cliënt in het kader van het certificeringproces voldoen aan de AVG en de UAVG. Als zodanig moet het in staat zijn het bewijs te leveren dat aan de eisen van het accreditatieproces is voldaan.

Het certificeringsorgaan levert het bewijs van naleving zoals vereist tijdens het accreditatieproces.

Dit houdt in ieder geval in dat het certificeringsorgaan aan de RvA bevestigt dat het niet onderworpen is aan een AP-onderzoek dat of regelgevende actie die zou kunnen inhouden dat het niet aan deze eis kan voldoen en als zodanig de accreditatie zou kunnen verhinderen.

4.1.2 Certificeringsovereenkomst

Het certificeringsorgaan dient naast de eisen van ISO 17065 aan te tonen dat zijn certificeringovereenkomsten:
1 vereisen dat de aanvrager altijd voldoet aan zowel de algemene certificeringseisen in de zin van 4.1.2.2.a van ISO 17065 als aan de criteria die door het AP of de EDPB overeenkomstig artikel 43, tweede lid, onder b), en artikel 42, vijfde lid, van de AVG zijn goedgekeurd;
2 vereisen dat de aanvrager de AP volledige transparantie biedt met betrekking tot de certificeringsprocedure, met inbegrip van al het vertrouwelijke materiaal, contractueel of anderszins, met betrekking tot de naleving van de gegevensbeschermingsvoorschriften overeenkomstig artikel 42, zevende lid, en artikel 58, eerste lid, onder c), van de AVG;

3 vereisen dat de aanvrager het certificeringsorgaan alle informatie en toegang tot zijn verwerkingsactiviteiten verstrekt die nodig zijn om de certificeringsprocedure overeenkomstig artikel 42, zesde lid, van de AVG uit te voeren;
4 vereisen dat de aanvrager de toepasselijke termijnen en procedures in acht neemt. In de certificeringsovereenkomst moet worden bepaald dat de termijnen en procedures die bijvoorbeeld voortvloeien uit het certificeringsmechanisme of andere regelgeving moeten worden gevolgd en nageleefd;
5 het certificeringsorgaan in staat stellen de redenen voor de toekenning of intrekking van de certificering overeenkomstig artikel 43, vijfde lid, van de AVG aan de AP bekend te maken, alsmede de informatie die de AP aan de EDPB zal moeten verstrekken om de EDPB in staat te stellen het certificeringsmechanisme op te nemen in een openbaar register overeenkomstig artikel 42, achtste lid, van de AVG;
6 regels bevatten over de noodzakelijke voorzorgsmaatregelen voor het onderzoek van klachten in de zin van 4.1.2.2 onder c nr. 2, en onder j, ook expliciete verklaringen bevatten over de structuur en de procedure voor de behandeling van klachten overeenkomstig artikel 43, tweede lid, onder d;
7 vereisen dat de aanvrager het certificeringsorgaan in kennis stelt van inbreuken op de AVG of de UAVG die door de AP en/of de gerechtelijke autoriteiten zijn vastgesteld en die van invloed kunnen zijn op de certificering zodra zij op de hoogte zijn van een dergelijke inbreuk;
8 met betrekking tot 4.1.2.2, onder c), punt 1, van ISO 17065 de regels voor geldigheid, verlenging en intrekking overeenkomstig artikel 42, zevende lid, en artikel 43, vierde lid, van de AVG vaststellen, met inbegrip van regels die passende termijnen vaststellen voor herbeoordeling of herziening overeenkomstig artikel 42, zevende lid, van de AVG en punt 7.9 van deze vereisten;
9 in aanvulling op de in punt 4.1.2.2 van ISO 17065 bedoelde minimumeisen, indien de gevolgen van de intrekking of opschorting van de accreditatie van het certificeringsorgaan gevolgen hebben voor de cliënt, ook de eventuele gevolgen voor de cliënt behandelen;
10 de verantwoordelijkheid van de aanvrager of de cliënt om, voor zover van toepassing, aan de AVG te voldoen, niet verminderen en geen afbreuk doen aan de taken en bevoegdheden van de bevoegde toezichthoudende autoriteiten overeenkomstig artikel 42, vijfde lid, van de AVG;
11 bindende evaluatiemethoden bevatten met betrekking tot de Target of Evaluation (ToE).

4.1.3 Gebruik van gegevensbeschermingszegels en -merken

Certificaten, zegels en merken mogen alleen worden gebruikt in overeenstemming met de artikelen 42 en 43 van de AVG en de richtsnoeren inzake accreditatie en certificering.

4.2 Omgaan met onpartijdigheid

In aanvulling op de eisen van ISO 17065, met name 3.13 en 4.2, moet het certificeringsorgaan aan de RvA aantonen:
1 dat het certificeringsorgaan voldoet aan de aanvullende eisen van de AP (overeenkomstig artikel 43, eerste lid, onder b), van de AVG) zoals uiteengezet in dit document;
2 dat in de certificering overeenkomstig artikel 43, tweede lid, onder a), van de AVG een afzonderlijk bewijs van zijn onafhankelijkheid wordt geleverd. Dit geldt met name voor het bewijs van de financiering van het certificeringsorgaan voor zover het de waarborging van de onpartijdigheid betreft;
3 dat de taken en verplichtingen van het certificeringsorgaan niet leiden tot een belangenconflict overeenkomstig artikel 43, tweede lid, onder e), van de AVG;
4 dat het certificeringsorgaan geen relevante banden heeft met de door hem beoordeelde aanvrager.

4.3 Aansprakelijkheid en financiering

In aanvulling op de eis in 4.3.1 van ISO 17065 moet het certificeringsorgaan regelmatig (d.w.z. eenmaal per jaar) aan het RvA aantonen over passende maatregelen te beschikken (bijvoorbeeld verzekering en/of reserves) om zijn aansprakelijkheden in de geografische regio's waar het actief is, te dekken. Voorts dient het certificeringsorgaan aan te tonen dat het financieel stabiel en onafhankelijk is. Het besluit met betrekking tot de selectie en de aanwijzing van de bewijsstukken valt onder de discretionaire bevoegdheid van de RvA.

4.4 Niet-discriminatoire voorwaarden

De eisen van 4.4 van ISO 17065 zijn van toepassing.

4.5 Vertrouwelijkheid

De eisen van 4.5 van ISO 17065 zijn van toepassing.

4.6 Openbare informatie

In aanvulling op de eisen in 4.6 van ISO 17065 moet het certificeringsorgaan aan de RvA aantonen dat:
1 alle (huidige en vorige) versies van de goedgekeurde criteria uit hoofde van artikel 42, vijfde lid, van de AVG worden gepubliceerd en gemakkelijk publiek toegankelijk zijn, en alsmede een toelichting op hoog niveau en op zinvolle wijze over de certificeringsprocedures en de desbetreffende geldigheidsperiode;
2 informatie over klachtenbehandelingsprocedures en beroepsprocedures openbaar worden gemaakt overeenkomstig artikel 43, tweede lid, onder d), van de AVG.

5 Eisen aan de structuur Artikel 43, vierde lid van de AVG ["juiste" beoordeling]

5.1 Organisatiestructuur en topmanagement

De eisen van 5.1 van ISO 17065 zijn van toepassing.

5.2 Mechanismen ter waarborging van onpartijdigheid

De eisen van 5.2 van ISO 17065 zijn van toepassing.

6 Eisen aan het personeel

6.1 Medewerkers van het certificeringsorgaan

In aanvulling op de eis in punt 6 van ISO 17065 moet het certificeringsorgaan aan de RvA aantonen dat zijn medewerkers:
1 blijk hebben gegeven van passende en voortdurende deskundigheid (kennis en ervaring) met betrekking tot gegevensbescherming overeenkomstig artikel 43, eerste lid, van de AVG;
2 onafhankelijk zijn en voortdurend over deskundigheid beschikken met betrekking tot het voorwerp van de certificering overeenkomstig artikel 43, tweede lid, onder a), van de AVG en geen belangenconflict hebben overeenkomstig artikel 43, tweede lid, onder e), van de AVG;
3 zich ertoe verbinden de in artikel 42, vijfde lid, van de AVG bedoelde criteria overeenkomstig artikel 43, tweede lid, onder b), van de AVG in acht te nemen;
4 aantoonbare, relevante en passende kennis van en ervaring met de toepassing van de gegevensbeschermingswetgeving hebben, waarbij de beoordelaars over meer specialistische deskundigheid en beroepservaring op het gebied van technische procedures (bijvoorbeeld audits en certificeringen) beschikken, terwijl de besluitvormers over meer algemene en uitgebreide deskundigheid en beroepservaring op het gebied van gegevensbescherming beschikken;
5 aantoonbare, relevante en passende kennis van en ervaring met technische en organisatorische maatregelen op het gebied van gegevensbescherming hebben;
6 aantoonbare ervaring hebben op de gebieden die in deze aanvullende eisen worden genoemd, in het bijzonder:

Voor medewerkers met technische expertise:
- Een kwalificatie op een relevant gebied van technische expertise hebben behaald op ten minste EKK-niveau[6] 6 of een erkende beschermde titel (bijvoorbeeld Dipl. Ing.) in het relevante gereglementeerde beroep, of een aanzienlijke relevante beroepservaring op dat gebied hebben.
- Medewerkers die verantwoordelijk zijn voor certificeringsbeslissingen moeten beschikken over aanzienlijke beroepservaring in het identificeren en uitvoeren van gegevensbeschermingsmaatregelen.
- Medewerkers die verantwoordelijk zijn voor evaluaties dienen te beschikken over beroepservaring op het gebied van technische gegevensbescherming en kennis van en ervaring met vergelijkbare procedures (bijvoorbeeld certificeringen/audits), en moeten, indien van toepassing, zijn geregistreerd.
- Medewerkers dienen aan te tonen dat zij domeinspecifieke kennis op het gebied van technische en auditvaardigheden op peil houden door middel van voortdurende professionele ontwikkeling.

Voor medewerkers met juridische expertise:
- Juridische studie aan een door de EU of de staat erkende universiteit gedurende ten minste acht semesters, met inbegrip van de academische graad Master (LL.M.) of gelijkwaardig, of significante beroepservaring.
- Medewerkers die verantwoordelijk zijn voor certificeringsbeslissingen dienen aan te tonen over significante beroepservaring te beschikken op het gebied van gegevensbeschermingsrecht en

[6] Zie het vergelijkingsinstrument voor het kwalificatiekader op https://ec.europa.eu/ploteus/en/compare?

dienen te zijn geregistreerd, voor zover van toepassing.
- Medewerkers die verantwoordelijk zijn voor de evaluaties dienen aan te tonen dat zij ten minste twee jaar beroepservaring hebben op het gebied van het gegevensbeschermingsrecht en kennis van en ervaring met vergelijkbare procedures (bijvoorbeeld certificeringen/audits), en dienen te zijn geregistreerd, voor zover van toepassing.
- Medewerkers dienen aan te tonen dat zij door middel van voortdurende professionele ontwikkeling domeinspecifieke kennis op het gebied van juridische en auditvaardigheden op peil houden.

6.2 Voorzieningen voor evaluatie

De eisen van 6.2 van ISO 17065 zijn van toepassing

7 Eisen aan de processen Artikel 43, tweede lid, onder c) en d), van de AVG.

7.1 Algemeen

In aanvulling op de vereiste in 7.1 van ISO 17065 moet de RvA het volgende waarborgen:
1 dat de certificeringsorganen aan deze aanvullende eisen voldoen (overeenkomstig artikel 43, eerste lid, onder b), van de AVG), zodat de taken en verplichtingen niet leiden tot een belangenconflict overeenkomstig artikel 43, tweede lid, onder e), van de AVG;
2 dat de bevoegde toezichthoudende autoriteit in kennis wordt gesteld voordat een certificeringsorgaan vanuit een nevenvestiging een goedgekeurd Europees gegevensbeschermingszegel in een nieuwe lidstaat in gebruik neemt.

7.2 Toepassing

In aanvulling op punt 7.2 van ISO 17065 eist het certificeringsorgaan dat de aanvraag:
1 een gedetailleerde beschrijving van de Target of Evaluation (ToE) bevat. Dit omvat ook interfaces en overdrachten naar andere systemen en organisaties, protocollen en andere waarborgen;
2 specificeert of er verwerkers worden gebruikt, en wanneer verwerkers de aanvrager zijn, worden hun verantwoordelijkheden en taken beschreven, en de aanvraag zal het (de) desbetreffende contract(en) voor de verwerkingsverantwoordelijken/verwerkers bevatten;
3 specificeert of gezamenlijke verwerkingsverantwoordelijken bij de verwerking betrokken zijn, en wanneer de gezamenlijke verwerkingsverantwoordelijke de aanvrager is, worden zijn verantwoordelijkheden en taken beschreven, en bevat de aanvraag de overeengekomen regeling; en
4 alle lopende of recente onderzoeken of regelgevende maatregelen van de AP bevat waaraan de aanvrager is onderworpen die relevant zijn gezien de reikwijdte van de certificering en de verwerking(en) waarop de certificering betrekking heeft.

7.3 Toetsing van de aanvraag

In aanvulling op punt 7.3 van ISO 17065:
- dient bij de beoordeling volgens punt 7.3, onder e), van ISO 17065 of er voldoende deskundigheid is, in passende mate rekening worden gehouden met zowel technische als juridische deskundigheid op het gebied van gegevensbescherming;
- dient bij de beoordeling van de aanvraag rekening te worden gehouden met de in punt 7.2, onder 4), van dit document genoemde controles op de naleving van de gegevensbeschermingsvoorschriften en dient het certificeringsorgaan zich ervan te vergewissen dat de aanvrager een geschikte kandidaat is voor certificering op het gebied van gegevensbescherming.

7.4 Evaluatie

In aanvulling op punt 7.4 van ISO 17065 moeten in het certificeringssysteem toereikende evaluatiemethoden worden beschreven om te beoordelen of de verwerkingshandeling(en) aan de certificeringscriteria voldoet (voldoen), met inbegrip van onderwerpen als:
1 een methode voor de beoordeling van de noodzaak en de evenredigheid van de verwerkingen gezien het doel en de betrokkenen;
2 een methode voor de evaluatie van de dekking, de samenstelling en de beoordeling van alle risico's die door de verwerkingsverantwoordelijke en de verwerker worden overwogen met betrekking tot de juridische gevolgen overeenkomstig de artikelen 30, 32 en 35 en 36 van de AVG en met betrekking tot de vaststelling van technische en organisatorische maatregelen overeenkomstig de artikelen 24, 25 en 32 van de AVG, voor zover de bovengenoemde artikelen van toepassing zijn op het voorwerp van de certificering, en
3 een methode voor de beoordeling van de middelen, waaronder garanties, voorzorgsmaatregelen en procedures, waarmee de bescherming van persoonsgegevens wordt gewaarborgd binnen de te

certificeren verwerkingen, en om aan te tonen dat wordt voldaan aan de wettelijke eisen zoals die in de vastgestelde criteria zijn vastgelegd; en

4 documenteren van methoden en bevindingen.

Het certificeringsorgaan dient erop toe te zien dat deze evaluatiemethoden worden gestandaardiseerd en consequent worden toegepast. Dit betekent dat vergelijkbare evaluatiemethoden worden gebruikt voor vergelijkbare ToE's. Elke afwijking van deze procedure moet door het certificeringsorgaan worden gemotiveerd.

In aanvulling op punt 7.4.2 van ISO 17065 mag de evaluatie worden uitgevoerd door onderaannemers die door het certificeringsorgaan zijn erkend, met gebruikmaking van dezelfde vereisten voor medewerkers vermeld in punt 6.

In aanvulling op punt 7.4.5 van ISO 17065 moet worden bepaald dat in het kader van een nieuwe evaluatie rekening mag worden gehouden met bestaande certificering, die betrekking heeft op hetzelfde voorwerp van de certificering. Het certificaat alleen is echter niet voldoende bewijs en het certificeringsorgaan is verplicht te controleren of aan de criteria met betrekking tot het voorwerp van de certificering wordt voldaan. Het volledige evaluatierapport en andere relevante informatie die een evaluatie van de bestaande certificering en de resultaten daarvan mogelijk maakt, worden in aanmerking genomen om tot een geïnformeerd besluit te komen.

Indien in het kader van een nieuwe evaluatie rekening wordt gehouden met bestaande certificering, dient de reikwijdte van die certificering ook in detail te worden beoordeeld met betrekking tot de naleving van de relevante certificeringscriteria.

In aanvulling op punt 7.4.6 van ISO 17065 moet het certificeringsorgaan in zijn certificeringregeling gedetailleerd vastleggen hoe de aanvrager door de in punt 7.4.6 vereiste informatie op de hoogte is van afwijkingen van de regeling. Dit omvat ten minste de aard en het tijdstip van deze informatie.

In aanvulling op punt 7.4.9 van ISO 17065 moet de evaluatiedocumentatie op verzoek volledig toegankelijk worden gemaakt voor de AP.

7.5 Herziening

In aanvulling op punt 7.5 van ISO 17065 zijn procedures voor de toekenning, regelmatige herziening en intrekking van de respectieve certificeringen overeenkomstig artikel 43, tweede en derde lid, van de AVG vereist.

7.6 Certificeringsbesluit

In aanvulling op punt 7.6.1 van ISO 17065 moet het certificeringsorgaan in zijn procedures gedetailleerd vastleggen hoe haar onafhankelijkheid en verantwoordelijkheden met betrekking tot individuele certificeringsbeslissingen worden gewaarborgd.

In aanvulling op punt 7.6 van ISO 17065 moet het certificeringsorgaan onmiddellijk vóór de afgifte of verlenging van de certificering de AP op de hoogte stellen door de ontwerp-goedkeuring, met inbegrip van de samenvatting van het evaluatierapport, aan de AP voor te leggen. In de samenvatting wordt duidelijk beschreven hoe aan de criteria wordt voldaan, zodat de redenen voor het verlenen of behouden van de certificering worden vermeld.

Naast de controle die wordt uitgevoerd in de aanvraagfase, voorafgaand aan de afgifte van de certificering, moet het certificeringsorgaan bij de aanvrager nagaan of er geen sprake is van een onderzoek of regelgevende maatregelen van de AP die de afgifte van de certificering zouden kunnen verhinderen.

7.7 Certificeringsdocumentatie

In aanvulling op punt 7.7.1, onder e), van ISO 17065 en in overeenstemming met artikel 42, zevende lid, van de AVG wordt vereist dat de geldigheidsduur van de certificeringen maximaal drie jaar bedraagt.

In aanvulling op punt 7.7.1, onder e), van ISO 17065 wordt vereist dat de periode van de voorgenomen monitoring in de zin van punt 7.9 van dit document wordt gedocumenteerd.

In aanvulling op punt 7.7.1, onder f), van ISO 17065 moet het certificeringsorgaan het voorwerp van de

certificering in de certificeringsdocumentatie vermelden (met vermelding van de versiestatus of soortgelijke kenmerken, indien van toepassing).

Bij de afgifte van het certificaat moet het certificeringsorgaan een kopie van de in punt 7.7.1 van ISO 17065 bedoelde certificeringsdocumentatie verstrekken aan de AP.

7.8 Repertorium van gecertificeerde producten

In aanvulling op punt 7.8 van ISO 17065 maakt het certificeringsorgaan een verslag van de afgegeven certificeringen publiek toegankelijk, met inbegrip van informatie over het certificeringsmechanisme en de geldigheidsduur van de certificeringen.

Het certificeringsorgaan stelt een samenvatting van het evaluatierapport ter beschikking aan het publiek. Het doel van deze samenvatting is om te helpen bij de transparantie over wat is gecertificeerd en hoe dit is beoordeeld. De volgende onderwerpen zullen worden toegelicht:
a) de reikwijdte van de certificering en een zinvolle beschrijving van het voorwerp van de certificering (ToE),
b) de respectieve certificeringscriteria (inclusief versie of functionele status),
c) de uitgevoerde evaluatiemethoden en tests en
d) het resultaat/de resultaten.

7.9 Toezicht

In aanvulling op de punten 7.9.1, 7.9.2 en 7.9.3 van ISO 17065 en overeenkomstig artikel 43, tweede lid, onder c), van de AVG zijn er regelmatig controlemaatregelen vereist om de certificering tijdens de controleperiode te behouden. Dergelijke maatregelen moeten risicogebaseerd en evenredig zijn en de maximale periode tussen de toezichtsactiviteiten mag niet meer dan 12 maanden bedragen.

7.10 Wijzigingen die van invloed zijn op de certificering

In aanvulling op de punten 7.10.1 en 7.10.2 van ISO 17065 moet het certificeringsorgaan ook rekening houden met wijzigingen die van invloed zijn op de certificering:
- elke inbreuk op persoonsgegevens, tenzij het onwaarschijnlijk is dat de inbreuk op persoonsgegevens leidt tot een risico voor de rechten en vrijheden van natuurlijke personen, of een door de AP en/of de gerechtelijke autoriteiten vastgestelde inbreuk op de AVG of de UAVG die verband houdt met het voorwerp van de certificering, gemeld door de opdrachtgever of de AP;
- wijzigingen in de gegevensbeschermingswetgeving;
- de vaststelling van gedelegeerde handelingen van de Europese Commissie overeenkomstig artikel 43, achtste lid, en artikel 43, negende lid, van de AVG;
- door het Europees Comité voor gegevensbescherming goedgekeurde documenten; en
- rechterlijke beslissingen met betrekking tot gegevensbescherming;
- wijzigingen in de stand van de techniek met betrekking tot gegevensbescherming of het voorwerp van de certificering.

De door het certificeringsorgaan uit te voeren wijzigingsprocedures omvatten onder meer: overgangsperioden, goedkeuringsproces met de AP, herbeoordeling van het relevante voorwerp van de certificering en passende maatregelen om de certificering in te trekken als de gecertificeerde verwerking niet langer in overeenstemming is met de bijgewerkte criteria.

7.11 Beëindiging, vermindering, opschorting of intrekking van de certificering

In aanvulling op punt 7.11.1 van ISO 17065 moet het certificeringsorgaan de AP en de RvA onverwijld schriftelijk informeren over de genomen maatregelen en over voortzetting, beperkingen, opschorting en intrekking van de certificering.

Indien de AP overeenkomstig artikel 58, tweede lid, onder h), van de AVG vaststelt dat niet of niet langer aan de eisen voor de certificering wordt voldaan, aanvaardt het certificeringsorgaan besluiten of bevelen om de certificering in te trekken of niet af te geven.

7.12 Registratie

In aanvulling op punt 7.12 van ISO 17065 is het certificeringsorgaan verplicht om alle documentatie volledig, begrijpelijk en up-to-date te houden en geschikt te maken voor audits.

7.13 Klachten en beroepsprocedures

In aanvulling op punt 7.13.1 van ISO 17065 moet het certificeringsorgaan het volgende beschrijven:
a) wie klachten of bezwaren kan indienen,
b) wie deze verwerkt bij het certificeringsorgaan,
c) welke verificaties in dit verband plaatsvinden; en
d) de mogelijkheden voor raadpleging van de belanghebbende partijen.

In aanvulling op punt 7.13.2 van ISO 17065 moet het certificeringsorgaan het volgende beschrijven:
a) hoe en aan wie een dergelijke bevestiging moet worden gegeven,
b) de termijnen hiervoor; en
c) welke processen daarna in gang worden gezet.

De certificeringsorganen maken hun klachtenbehandelingsprocedures openbaar en gemakkelijk toegankelijk voor de betrokkenen.

Het certificeringsorgaan is verplicht de indiener van een klacht zonder onnodige vertraging en in ieder geval binnen een maand na ontvangst van de klacht op de hoogte te stellen van de voortgang en/of het resultaat van de klacht. Deze termijn kan zo nodig worden verlengd. In dat geval deelt het certificeringsorgaan de indiener van de klacht binnen een maand na ontvangst van het verzoek mee wanneer het resultaat kan worden verwacht.

In aanvulling op punt 7.13.1 van ISO 17065 moet het certificeringsorgaan bepalen hoe de scheiding tussen certificeringactiviteiten en de behandeling van beroepsprocedures en klachten wordt gewaarborgd.

8 Eisen aan het managementsysteem

In aanvulling op hoofdstuk 8 van ISO 17065 moeten de managementbeginselen en de gedocumenteerde uitvoering ervan transparant zijn en door het geaccrediteerde certificeringsorgaan in de accreditatieprocedure overeenkomstig artikel 58 van de AVG en vervolgens op verzoek van de AP op elk moment tijdens een onderzoek worden bekendgemaakt in de vorm van gegevensbeschermingscontroles overeenkomstig artikel 58, eerste lid, onder b), van de AVG of een herziening van de overeenkomstig artikel 42, zevende lid, van de AVG afgegeven certificeringen overeenkomstig artikel 58, eerste lid, onder c), van de AVG.

De procedures in geval van opschorting of intrekking van de accreditatie worden geïntegreerd in het managementsysteem van het certificeringsorgaan, met inbegrip van de kennisgeving aan hun klanten en aanvragers.

Het certificeringsorgaan stelt een klachtenbehandelingsproces met de nodige niveaus van onafhankelijkheid vast als integraal onderdeel van het managementsysteem, waarmee met name de eisen van punt 4.1.2.2, onder c), punt 4.1.2.2, onder j), punt 4.6, onder d), en punt 7.13 van ISO 17065 worden uitgevoerd.

8.1 Algemene eisen voor het managementsysteem

De eisen van 8.1 Opties van ISO 17065 zijn van toepassing.

8.2 Documentatie voor het managementsysteem

De eisen van 8.2 van ISO 17065 zijn van toepassing.

8.3 Controle van documenten

De eisen van 8.3 van ISO 17065 zijn van toepassing.

8.4 Controle van dossiers

De eisen van 8.4 van ISO 17065 zijn van toepassing.

8.5 Managementbeoordeling

De eisen van 8.5 van ISO 17065 zijn van toepassing.

8.6 Interne audits

De eisen van 8.6 van ISO 17065 zijn van toepassing.

8.7 Corrigerende acties

De eisen van 8.7 van ISO 17065 zijn van toepassing.

8.8 Preventieve acties

De eisen van 8.8 van ISO 17065 zijn van toepassing.

9. Verdere aanvullende eisen

9.1 Actualiseren van de evaluatiemethoden

Het certificeringsorgaan stelt procedures vast voor de bijwerking van de evaluatiemethoden voor de toepassing in het kader van de evaluatie overeenkomstig punt 7.4 van ISO 17065 en onderhavig document. De bijwerking moet plaatsvinden in het kader van wijzigingen in het wettelijk kader, 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 stellen procedures vast om de opleiding van hun werknemers te waarborgen met het oog op de actualisering van hun vaardigheden, rekening houdend met de in punt 9.1 van dit document vermelde ontwikkelingen.

9.3 Verantwoordelijkheden en competenties

9.3.1 Communicatie tussen het certificeringsorgaan en zijn cliënten en aanvragers

Er dienen procedures te worden vastgesteld voor de toepassing van passende procedures en communicatiestructuren tussen het certificeringsorgaan en zijn cliënt of aanvrager. Dit omvat:

1 Het bijhouden van documentatie over de taken en verantwoordelijkheden van het geaccrediteerde certificeringsorgaan, met het oog op
   - het beantwoorden van informatieverzoeken; of
   - om contact op te nemen in geval van een klacht over een certificering.

2 Het onderhouden van een aanvraagprocedure met het oog op
   - informatie over de status en het resultaat van een aanvraag;
   - evaluaties door de AP met betrekking tot
     - terugkoppeling;
     - beslissingen van de AP.

9.3.2 Documentatie van de evaluatieactiviteiten

Er gelden geen aanvullende eisen.

9.3.3 Behandeling van klachten

Als integraal onderdeel van het managementsysteem wordt een klachtenbehandelingsprocedure vastgesteld, waarmee name de eisen van punt 4.1.2.2, onder c), punt 4.1.2.2, onder j), punt 4.6, onder d), en punt 7.13 van ISO 17065 moeten worden uitgevoerd.

Relevante klachten en bezwaren moeten met de AP worden gedeeld.

9.3.4. Management van intrekking

De procedures in geval van schorsing of intrekking van de accreditatie worden geïntegreerd in het managementsysteem van het certificeringsorgaan, met inbegrip van de kennisgeving aan cliënten.