Richtsnoeren van 1/2018 voor certificering en het vaststellen van certificeringscriteria overeenkomstig de artikelen 42 en 43 van de verordening

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	Opname van bijlage 2 (versie 2.0 van bijlage 2 vastgesteld op 4 juni 2019 na een openbare raadpleging)
Versie 2.1	9 april 2019	Vaststelling van een rectificatie van de richtsnoeren (artikel 45)
Versie 2.0	23 januari 2019	Vaststelling van de richtsnoeren na een openbare raadpleging - Op dezelfde datum is bijlage 2 (versie 1.0) vastgesteld voor een openbare raadpleging
Versie 1.0	25 mei 2018	Vaststelling van de richtsnoeren voor een openbare raadpleging

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 (hierna "AVG" genoemd),

Gezien de EER-overeenkomst en in het bijzonder bijlage XI bij, en protocol 37 van die overeenkomst, als gewijzigd bij Besluit nr. 154/2018 van het Gemengd Comité van de EER van 6 juli 2018,

Gezien de artikelen 12 en 22 van het reglement van orde van het Gemengd Comité van de EER van 25 mei 2018,

In het licht van de uitkomsten van de openbare raadpleging over de richtsnoeren, die plaatsvond tussen 30 mei 2018 en 12 juli 2018 en over bijlage 2, die plaatsvond tussen 15 februari 2019 en 29 maart 2019, overeenkomstig artikel 70, lid 4, van de AVG

HEEFT DE VOLGENDE RICHTSNOEREN VASTGESTELD

1 INLEIDING

1. De algemene verordening gegevensbescherming (Verordening (EU) 2016/679, "de AVG" of "de Verordening") voorziet in een gemoderniseerd kader voor gegevensbescherming in Europa, waarin het verantwoordingsbeginsel en grondrechten een belangrijke rol spelen. Binnen dit kader staan maatregelen centraal die naleving van de bepalingen van de AVG makkelijker moeten maken. Daartoe behoren verplichte vereisten voor concrete omstandigheden (waaronder de benoeming van functionarissen voor gegevensbescherming en de uitvoering van gegevensbeschermingseffectbeoordelingen) en vrijwillige maatregelen, zoals gedragscodes en certificeringsmechanismen.

2. Voordat de AVG werd vastgesteld, heeft de Groep artikel 29 geconstateerd dat certificering een belangrijke rol zou kunnen spelen binnen het verantwoordingskader voor gegevensbescherming1. Certificering moet een betrouwbaar bewijs van de naleving van gegevensbescherming leveren en daarvoor zijn duidelijke regels voor het verlenen van certificeringen nodig2. Artikel 42 van de AVG biedt een rechtsgrond voor de ontwikkeling van zulke regels.

3. Artikel 42, lid 1, AVG luidt:

   "De lidstaten, de toezichthoudende autoriteiten, het [Europees] Comité [voor gegevensbescherming] en de Commissie bevorderen, met name op Unieniveau, de invoering van certificeringsmechanismen voor gegevensbescherming en gegevensbeschermingszegels en -merktekens waarmee kan worden aangetoond dat verwerkingsverantwoordelijken en

[1] Groep artikel 29, advies 3/2010 over het verantwoordingsbeginsel (WP173), 13 juli 2010, punten 69-71.
[2] Groep artikel 29, advies 3/2010 over het verantwoordingsbeginsel (WP173), punt 69.

verwerkers bij verwerkingen in overeenstemming met deze verordening handelen. Er wordt ook rekening gehouden met de specifieke behoeften van kleine, middelgrote en micro-ondernemingen".

4. Certificeringsmechanismen3 kunnen de transparantie voor betrokkenen verbeteren, maar ook binnen zakelijke relaties, bijvoorbeeld tussen verwerkingsverantwoordelijken en verwerkers, helderheid scheppen. In overweging 100 van de AVG staat dat het instellen van certificeringsmechanismen de transparantie en naleving van de verordening kan versterken, zodat betrokkenen snel het gegevensbeschermingsniveau van producten en diensten ter zake kunnen beoordelen4.

5. Met de AVG wordt geen recht op of een verplichting tot certificering voor verwerkingsverantwoordelijken en verwerkers ingevoerd. Overeenkomstig artikel 42, lid 3, is certificering vrijwillig en kan daarmee worden aangetoond dat in overeenstemming met de AVG is gehandeld. Lidstaten en toezichthoudende autoriteiten worden opgeroepen het instellen van certificeringsmechanismen te bevorderen en moeten de rol van de betrokkene in het certificeringsproces en de levenscyclus vaststellen.

6. Bovendien moeten toezichthoudende autoriteiten de aansluiting bij goedgekeurde certificeringsmechanismen als een verzwarende of verzachtende factor in aanmerking nemen bij het nemen van besluiten over de vraag of een administratieve geldboete wordt opgelegd en over de hoogte daarvan (artikel 83, lid 2, onder j)5.

1.1 Toepassingsgebied van de richtsnoeren

7. Deze richtsnoeren hebben een beperkt toepassingsgebied. Zij moeten niet worden gezien als een procedurehandleiding voor certificering overeenkomstig de AVG. De richtsnoeren moeten primair fungeren als overkoepelende vereisten en criteria die relevant kunnen zijn voor alle soorten certificeringsmechanismen die overeenkomstig de artikelen 42 en 43 AVG worden opgesteld. Daartoe hebben de richtsnoeren de volgende doelen:

   - de grondslag onderzoeken voor certificering als instrument voor verantwoording;
   - de sleutelbegrippen verklaren van de certificeringsbepalingen van de artikelen 42 en 43; en
   - het toepassingsgebied verklaren van wat op grond van de artikelen 42 en 43 kan worden gecertificeerd en van de certificeringsdoelstelling;
   - een begrijpelijke, ondubbelzinnige, ofwel zo reproduceerbaar mogelijke, en vergelijkbare uitkomst van de certificering bevorderen, ongeacht het certificeringsorgaan (vergelijkbaarheid).

[3] In deze richtsnoeren worden certificeringsmechanismen en gegevensbeschermingszegels en -merktekens gezamenlijk certificeringsmechanismen genoemd, zie paragraaf 1.3.2.
[4] In overweging 100 staat dat het instellen van certificeringsmechanismen moet worden bevorderd om "de transparantie en naleving van de verordening te versterken […], zodat betrokkenen snel het gegevensbeschermingsniveau van producten en diensten ter zake kunnen beoordelen".
[5] Zie Groep artikel 29, richtsnoeren voor de toepassing en vaststelling van administratieve geldboeten in de zin van Verordening (EU) 2016/679 (WP 253).

8. De AVG biedt lidstaten en toezichthoudende autoriteiten een aantal mogelijkheden om de artikelen 42 en 43 uit te voeren. De richtsnoeren geven advies over de interpretatie en uitvoering van de bepalingen van de artikelen 42 en 43 en helpen lidstaten, toezichthoudende autoriteiten en nationale accreditatie-instanties de uitvoering van certificeringsmechanismen in overeenstemming met de AVG op een meer consistente en geharmoniseerde wijze te benaderen.

9. Het advies uit de richtsnoeren is van belang voor:

   - bevoegde toezichthoudende autoriteiten en het Europees Comité voor gegevensbescherming (het "EDPB"), met het oog op de goedkeuring van certificeringscriteria overeenkomstig artikel 42, lid 5, artikel 58, lid 3, onder f), en artikel 70, lid 1), onder o);
   - certificeringsorganen, met het oog op het opstellen en herzien van certificeringscriteria, alvorens deze ter goedkeuring aan de bevoegde toezichthoudende autoriteit worden voorgelegd, overeenkomstig artikel 42, lid 5;
   - het EDPB, met het oog op de goedkeuring van een Europees gegevensbeschermingszegel overeenkomstig artikel 42, lid 5, en artikel 70, lid 1, onder o);
   - toezichthoudende autoriteiten, met het oog op het opstellen van eigen certificeringscriteria;
   - de Europese Commissie, die bevoegd is gedelegeerde handelingen vast te stellen met het oog op de nadere invulling van de in aanmerking te nemen eisen voor de in artikel 43, lid 8, bedoelde certificeringsmechanismen;
   - het EDPB, met het oog op het uitbrengen van een advies ten behoeve van de Europese Commissie over de in artikel 70, lid 1, onder q), en artikel 43, lid 8, bedoelde certificeringseisen;
   - nationale accreditatie-instanties, die met het oog op de accreditatie van certificeringsorganen in overeenstemming met EN-ISO/IEC 17065/2012 certificeringscriteria en in overeenstemming met artikel 43 aanvullende vereisten in aanmerking moeten nemen; en
   - verwerkingsverantwoordelijken en verwerkers, met het oog op de vaststelling van hun eigen strategie voor het naleven van de AVG en certificering als een manier om de naleving ervan te kunnen aantonen.

10. Het EDPB zal met afzonderlijke richtsnoeren komen voor de vaststelling van criteria voor de goedkeuring van certificeringsmechanismen als instrument voor de doorgifte aan derde landen of internationale organisaties overeenkomstig artikel 42, lid 2.

1.2 Het doel van certificering volgens de AVG

11. Artikel 42, lid 1, bepaalt dat certificeringsmechanismen moeten worden vastgesteld, "waarmee kan worden aangetoond dat verwerkingsverantwoordelijken en verwerkers bij verwerkingen in overeenstemming met deze verordening handelen".

12. De AVG beschrijft het kader waarin goedgekeurde certificeringsmechanismen kunnen worden gebruikt als een element om aan te tonen dat verwerkingsverantwoordelijken en verwerkers aan verplichtingen voldoen betreffende:

    - het uitvoeren en aantonen van passende technische en organisatorische maatregelen, als bedoeld in artikel 24, leden 1, 3 en 25, en artikel 32, leden 1 en 3;
    - voldoende garanties (tussen verwerker en verwerkingsverantwoordelijke), als bedoeld in lid 1 en (tussen subverwerker en verwerker) lid 4 van het artikel waarnaar wordt verwezen in artikel 28, lid 5.

13. Aangezien certificering op zich geen bewijs is van overeenstemming, maar eerder een element is dat kan worden gebruikt om overeenstemming aan te tonen, moet certificering op een transparante wijze verlopen. Om overeenstemming aan te tonen, is ondersteunende documentatie nodig. Dit zijn speciaal geschreven verslagen waarin de criteria niet alleen worden herhaald, maar ook wordt beschreven hoe eraan wordt voldaan. Indien niet aan de criteria is voldaan, moet erin worden beschreven welke correcties en corrigerende maatregelen van toepassing zijn en in hoeverre die gepast zijn. Deze informatie vormt de grondslag voor de toekenning van de certificering en het behoud ervan. Daartoe behoort tevens de uiteenzetting van het individuele besluit om een certificaat af te geven, te verlengen of in te trekken. Hierin moeten de redenen, argumenten en bewijzen die het gevolg zijn van de toepassing van criteria, en de conclusies, oordelen of gevolgtrekkingen uit feiten en veronderstellingen die tijdens de certificering aan het licht zijn gekomen, worden opgenomen.

1.3 Basisbegrippen

14. In de volgende paragraaf worden de basisbegrippen uit de artikelen 42 en 43 nader bekeken. Aan de hand van deze analyse worden de basistermen en het toepassingsgebied van de certificering volgens de AVG inzichtelijk gemaakt.

1.3.1 Interpretatie van "certificering"

15. De AVG geeft geen definitie van "certificering". De Internationale Organisatie voor normalisatie (ISO) geeft als universele definitie voor certificering "het afgeven door een onafhankelijke instantie van een schriftelijke verzekering (een certificaat) dat een product, dienst of systeem aan specifieke vereisten voldoet." Certificering staat ook wel bekend als "conformiteitsbeoordeling door derden" en certificeringsorganen worden ook wel aangeduid als "conformiteitsbeoordelingsinstanties". In EN-ISO/IEC 17000:2004 –

Conformiteitsbeoordeling – Verklarende woordenlijst en algemene principes (waarnaar ISO 17065 verwijst) – wordt de volgende definitie van certificering gegeven: "attestering door derden […] met betrekking tot producten, processen en diensten".

16. Attestering is een "afgifte van een attest, op basis van een na een beoordeling genomen besluit, waarin wordt bevestigd dat is aangetoond dat aan de gestelde eisen is voldaan" (paragraaf 5.2, ISO 17000:2004).

17. In het kader van certificering overeenkomstig de artikelen 42 en 43 van de AVG, moet certificering verwijzen naar attestering door derden in verband met door verwerkingsverantwoordelijken en verwerkers uitgevoerde verwerkingen.

1.3.2 Certificeringsmechanismen, zegels en merktekens

18. Er wordt in de AVG geen definitie gegeven van "certificeringsmechanismen, zegels of merktekens" en de termen worden gezamenlijk gebruikt. Een certificaat is een verklaring van conformiteit. Een zegel of merkteken kan worden gebruikt om aan te geven dat de certificeringsprocedure succesvol is afgerond. Een zegel of merkteken verwijst veelal naar een logo of symbool, waarmee (in aanvulling op een certificaat) wordt aangegeven dat het voorwerp van certificering onafhankelijk is beoordeeld in een certificeringsprocedure en voldoet aan specifieke vereisten die zijn vastgelegd in normatieve documenten, zoals voorschriften, normen of technische specificaties. Deze vereisten voor certificering volgens de AVG maken deel uit van de aanvullende vereisten waarmee de regels voor accreditatie van certificeringsorganen in EN-ISO/IEC 17065/2012 zijn uitgebreid en de certificeringscriteria die door de bevoegde toezichthoudende autoriteit of het Comité zijn goedgekeurd. Een certificaat, zegels of merkteken kan alleen op grond van de AVG worden afgegeven na de onafhankelijke beoordeling van bewijs door een geaccrediteerd certificeringsorgaan of een bevoegde toezichthoudende autoriteit, waaruit blijkt dat aan de certificeringscriteria is voldaan.

19. De tabel geeft een algemeen voorbeeld van een certificeringsproces.

Indiening van aanvraag door verwerkingsverantwoordelijke of verwerker	Formele controle door CO	Beoordeling Voorevaluatie	Beoordeling Evaluatie van OvB	Beoordeling Validatie van resultaten	Mededeling aan bevoegde toezichthoudende autoriteit	Certificering	Toezicht	Verlenging van certificering
Is de beschrijving van het onderwerp van beoordeling eenduidig en volledig, inclusief interfaces?	Kan de beschrijving van het onderwerp van beoordeling worden aanvaard?	Welke criteria zijn van toepassing?	Voldoet het onderwerp van beoordeling aan de criteria?	Komt het onderwerp van beoordeling in alle relevante gespecificeerde criteria terug?	Zijn de redenen voor afgifte of intrekking van de certificering vermeld?	Kan de certificering worden toegekend?	Voldoet het onderwerp van beoordeling nog altijd aan de criteria?	Voldoet de verwerking nog altijd aan de certificeringscriteria?
Kan toegang worden verleend aan de verwerkingsactiviteiten voor het onderwerp van beoordeling?	Zijn alle documenten volledig en bijgewerkt?	Welke evaluatiemethoden zijn van toepassing?	Is het onderwerp van beoordeling goed gedocumenteerd?	Is de evaluatie voldoende gedocumenteerd?		Zijn de verslagen klaar voor publicatie?	Is het certificaat/zegel/merkteken op juiste wijze gebruikt?	Zijn ontwikkelingsgebieden naar behoren aangepakt?
Artikel 42, lid 6	Artikel 43, lid 4	Artikel 43, lid 4	Artikel 42, lid 5, Artikel 43, lid 4	Artikel 43, lid 4	Artikel 43, lid 1, Artikel 43, lid 5	Artikel 43, lid 1, Artikel 42, lid 7	Artikel 42, lid 7	Artikel 42, lid 7

2 DE ROL VAN DE TOEZICHTHOUDENDE AUTORITEITEN

20. Artikel 42, lid 5, bepaalt dat certificering moet worden afgegeven door een geaccrediteerd certificeringsorgaan of een bevoegde toezichthoudende autoriteit. De AVG ziet de afgifte van certificeringen niet als een verplichte taak van de toezichthoudende autoriteiten. In plaats daarvan voorziet de AVG in een aantal verschillende modellen. Zo kan een toezichthoudende autoriteit een of meer van de volgende mogelijkheden kiezen:

    - zelf een certificering afgeven, volgens haar eigen certificeringsregeling;
    - zelf een certificering afgeven, volgens haar eigen certificeringsregeling, waarbij de beoordelingsprocedure volledig of gedeeltelijk aan derden wordt toevertrouwd;
    - zelf een certificeringsregeling opstellen en de certificering en afgifte van certificering aan certificeringsorganen toevertrouwen; en
    - de markt stimuleren om certificeringsmechanismen te ontwikkelen.

21. Toezichthoudende autoriteiten moeten ook hun eigen rol tegen de achtergrond zien van de besluiten die op nationaal niveau ten aanzien van accreditatiemechanismen worden genomen. Dit geldt in het bijzonder indien de toezichthoudende autoriteit zelf bevoegd is om overeenkomstig artikel 43, lid 1, AVG certificeringsorganen te accrediteren. Elke toezichthoudende autoriteit zal zo haar eigen benadering kiezen om de certificering in het brede perspectief van de AVG te kunnen uitvoeren. Deze keuze zal niet alleen worden gemaakt op basis van de taken en bevoegdheden uit de artikelen 57 en 58, maar ook vanuit de opvatting dat certificering een rol speelt bij de vaststelling van administratieve geldboeten en meer in het algemeen als instrument om overeenstemming aan te tonen.

2.1 De toezichthoudende autoriteit als certificeringsorgaan

22. Wanneer een toezichthoudende autoriteit certificeringen wil gaan uitvoeren, zal zij haar rol in het licht van de taken die haar op grond van de AVG toekomen, zorgvuldig moeten beoordelen. Zij zal bij de uitvoering van haar taken op een transparante wijze te werk moeten gaan. Dat betekent dat zij er in het bijzonder op moet letten bevoegdheden ten aanzien van onderzoek en handhaving te scheiden om mogelijke belangenconflicten te voorkomen.

23. In haar functie als certificeringsorgaan zal de toezichthoudende autoriteit een gedegen certificeringsmechanisme moeten opstellen en haar eigen certificeringscriteria moeten ontwikkelen of vaststellen. Bovendien moet elke toezichthoudende autoriteit die certificeringen afgeeft, deze certificeringen periodiek toetsen (artikel 57, lid 1, onder o)) en heeft zij de bevoegdheid deze in te trekken indien niet langer aan de certificeringsvereisten wordt voldaan (artikel 58, lid 2, onder h)). Om aan deze vereisten te voldoen, is het zinvol een certificeringsprocedure en procedure-eisen op te stellen en, tenzij anders bepaald in bijvoorbeeld nationale wetgeving, met de individuele aanvragende organisatie een juridisch bindende overeenkomst betreffende het uitvoeren van certificeringsactiviteiten te sluiten. Daarbij is het van belang dat de aanvrager zich op grond van deze certificeringsovereenkomst ten minste aan de certificeringscriteria moet houden, waaronder

noodzakelijke regelingen voor het uitvoeren van beoordelingen, het uitoefenen van toezicht op de naleving van de criteria en periodieke toetsing, inclusief de toegang tot informatie en/of gebouwen, het documenteren en publiceren van verslagen en resultaten en het onderzoeken van klachten. Bovendien wordt van een toezichthoudende autoriteit verwacht dat zij zich in aanvulling op de vereisten van artikel 43, lid 2, aan de vereisten van de richtsnoeren voor accreditatie van certificeringsorganen houdt.

2.2 Aanvullende certificeringstaken van de toezichthoudende autoriteit

24. In lidstaten met actieve certificeringsorganen heeft de toezichthoudende autoriteit, ongeacht haar eigen activiteiten, de bevoegdheid en taak om:

    - de criteria van een certificeringsregeling te beoordelen en een ontwerpbesluit op te stellen (artikel 42, lid 5);
    - het Comité het ontwerpbesluit mee te delen, indien het voornemens is de criteria voor certificering goed te keuren (artikel 64, lid 1, onder c), en artikel 64, lid 7) en rekening te houden met het advies van het Comité (artikel 64, lid 1, onder c), en artikel 70, lid 1, onder t));
    - de certificeringscriteria goed te keuren (artikel 58, lid 3, onder f)), alvorens de accreditatie en de certificering kunnen plaatsvinden (artikel 42, lid 5, en artikel 43, lid 2, onder b));
    - de certificeringscriteria openbaar te maken (artikel 43, lid 6);
    - op te treden als bevoegde autoriteit voor EU-brede certificeringsregelingen, die kunnen leiden tot een EDPB-goedgekeurd Europees gegevensbeschermingszegel (artikel 42, lid 5, en artikel 70, lid 1, onder o)); en
    - een certificeringsorgaan te gelasten om a) geen certificering af te geven of b) een certificering in te trekken indien niet of niet langer aan de certificeringsvereisten (certificeringsprocedures of -criteria) wordt voldaan (artikel 58, lid 2, onder h)).

25. De AVG geeft de toezichthoudende autoriteit de taak om certificeringscriteria goed te keuren, maar niet om criteria te ontwikkelen. Om certificeringscriteria overeenkomstig artikel 42, lid 5, goed te keuren, moet de toezichthoudende autoriteit duidelijk inzicht hebben in wat kan worden verwacht. Dit geldt met name qua toepassingsgebied en inhoud voor het aantonen van de overeenstemming met de AVG en ten aanzien van haar taak toe te zien op de toepassing van de verordening en de handhaving daarvan. De bijlage bevat richtsnoeren voor een geharmoniseerde benadering van de beoordeling van criteria met het oog op goedkeuring.

26. Overeenkomstig artikel 43, lid 1, moeten certificeringsorganen, alvorens zij overgaan tot de afgifte of verlenging van certificeringen, hun toezichthoudende autoriteit op de hoogte stellen om haar in de gelegenheid te stellen haar corrigerende bevoegdheden overeenkomstig artikel 58, lid 2, onder h), uit te oefenen. Bovendien moeten de certificeringsorganen de bevoegde toezichthoudende autoriteit overeenkomstig artikel 43,

lid 5, op de hoogte stellen van de redenen voor het afgeven of het intrekken van de aangevraagde certificering. Hoewel toezichthoudende autoriteiten op grond van de AVG kunnen bepalen hoe zij deze informatie in de praktijk willen ontvangen, erkennen, toetsen en afhandelen (bijvoorbeeld door middel van technologische oplossingen om rapportage door certificeringsorganen mogelijk te maken), kunnen een procedure en criteria voor de verwerking van informatie en verstrekte verslagen over succesvolle certificeringsprojecten door het certificeringsorgaan overeenkomstig artikel 43, lid 1, worden opgesteld. Op basis van deze informatie kan de toezichthoudende autoriteit haar bevoegdheid uitoefenen om een certificeringsorgaan te gelasten een certificering in te trekken of geen certificering af te geven (artikel 58, lid 2, onder h)) en om toe te zien op de toepassing van de vereisten en de certificeringscriteria en deze te handhaven overeenkomstig de AVG (artikel 57, lid 1, onder a), en artikel 58, lid 2, onder h)). Dit draagt bij aan een geharmoniseerde benadering en vergelijkbaarheid van de certificering door verschillende certificeringsorganen en zal ervoor zorgen dat informatie over de certificeringsstatus van een organisatie bekend is bij toezichthoudende autoriteiten.

3 DE ROL VAN CERTIFICERINGSORGANEN

27. Certificeringsorganen moeten certificeringen afgeven, beoordelen, verlengen en intrekken (artikel 42, leden 5 en 7) aan de hand van een certificeringsmechanisme en goedgekeurde criteria (artikel 43, lid 1). Daarom moet het certificeringsorgaan of de eigenaar van een certificeringsregeling certificeringscriteria en certificeringsprocedures vaststellen en opstellen, waaronder procedures voor toezicht op de naleving, beoordeling, klachtafhandeling en intrekking. De certificeringscriteria worden beoordeeld als onderdeel van de accreditatieprocedure, waarin rekening wordt gehouden met de regels en procedures voor de afgifte van certificeringen, zegels of merktekens (artikel 43, lid 2, onder c)).

28. Om als certificeringsorgaan overeenkomstig artikel 43 een accreditatie te kunnen verkrijgen, moeten een certificeringsmechanisme en certificeringscriteria bestaan. Van grote invloed op het handelen van een certificeringsorgaan zijn het toepassingsgebied en de aard van het certificeringscriterium, die gevolgen hebben voor de certificeringsprocedures en andersom. Op basis van specifieke criteria kunnen bijvoorbeeld speciale beoordelingsmethoden worden verlangd, zoals inspecties ter plaatse en codebeoordelingen. Deze procedures zijn verplicht voor accreditatie en worden in de richtsnoeren voor accreditatie nader toegelicht.

29. Op grond van de AVG moet het certificeringsorgaan toezichthoudende autoriteiten van informatie voorzien, met name wat betreft individuele certificeringen. Dit is nodig om toezicht te kunnen houden op de toepassing van het certificeringsmechanisme (artikel 42, lid 7, artikel 43, lid 5, en artikel 58, lid 2, onder h)).

4 GOEDKEURING VAN CERTIFICERINGSCRITERIA

30. De certificeringscriteria maken integraal deel uit van certificeringsmechanismen. De AVG vereist daarom dat certificeringscriteria van een certificeringsmechanisme worden goedgekeurd door de bevoegde toezichthoudende autoriteit (artikel 42, lid 5, en artikel 43,

lid 2, onder b)). In het geval van een Europees gegevensbeschermingszegel moeten de certificeringscriteria worden goedgekeurd door het EDPB (artikel 42, lid 5, en artikel 70, lid 1, onder o)). Beide trajecten voor de goedkeuring van certificeringscriteria worden hieronder nader toegelicht.

31. Het EDPB erkent de goedkeuring van certificeringscriteria om de volgende redenen:

    - het naar behoren tot uiting brengen van de vereisten en beginselen betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens uit Verordening (EU) 2016/679; en
    - het bijdragen aan een consequentie toepassing van de AVG.

32. Goedkeuring wordt verleend op basis van de vereiste uit de AVG dat het certificeringsmechanisme dat verwerkingsverantwoordelijken en verwerkers in staat moet stellen de naleving van de AVG aan te tonen, volledig tot uiting komt in de certificeringscriteria.

4.1 Goedkeuring van criteria door de bevoegde toezichthoudende autoriteit

33. Voorafgaand aan of tijdens de accreditatieprocedure voor een certificeringsorgaan moet de bevoegde toezichthoudende autoriteit de certificeringscriteria goedkeuren. Goedkeuring is ook vereist voor geactualiseerde of aanvullende regelingen of reeksen van criteria volgens ISO 17065 van hetzelfde certificeringsorgaan, alvorens gebruik wordt gemaakt van de gewijzigde certificeringsmechanismen (artikel 42, lid 5, en artikel 43, lid 2, onder b)). Toezichthoudende autoriteiten moeten alle goedkeuringsverzoeken voor certificeringscriteria op een eerlijke en niet-discriminerende wijze behandelen. Daarbij moeten zij een openbare procedure volgen, waarin de algemene voorwaarden waaraan moet worden voldaan, worden gespecificeerd en de goedkeuringsprocedure wordt beschreven.

34. Certificeringsorganen kunnen alleen certificeringen afgeven in een bepaalde lidstaat, overeenkomstig de door de toezichthoudende autoriteit in de betreffende lidstaat goedgekeurde criteria. Certificeringscriteria moeten met andere woorden worden goedgekeurd door de bevoegde toezichthoudende autoriteit in de lidstaat waar het certificeringsorgaan certificeringen wil gaan afgeven en de accreditatie verkrijgt. In de volgende paragraaf staat informatie over EU-brede certificeringsregelingen.

4.2 Goedkeuring van criteria door het EDPB voor een Europees gegevensbeschermingszegel

35. Certificeringsorganen kunnen ook certificeringen afgeven in overeenstemming met door het EDPB goedgekeurde criteria voor een Europees gegevensbeschermingszegel. Overeenkomstig artikel 63 door het EDPB goedgekeurde certificeringscriteria kunnen leiden tot een Europees gegevensbeschermingszegel (artikel 42, lid 5). Gezien bestaande afspraken over certificering en accreditatie erkent het EDPB dat het wenselijk is om te voorkomen dat

de markt voor certificering van gegevensbescherming versnipperd raakt. Het EDPB merkt op dat lidstaten, toezichthoudende autoriteiten, het Comité en de Commissie overeenkomstig artikel 42, lid 1, de vaststelling van certificeringsmechanismen moeten bevorderen, met name op Unieniveau.

4.2.1 Goedkeuringsaanvraag

36. De aanvraag voor goedkeuring van criteria overeenkomstig artikel 42, lid 5, en artikel 70, lid 1, onder o), door het EDPB, moet worden ingediend via een bevoegde toezichthoudende autoriteit en moet de reden van de eigenaar van een regeling, de kandidaat of het geaccrediteerde certificeringsorgaan bevatten waarom de criteria tot een certificeringsmechanisme voor verwerkingsverantwoordelijken en verwerkers in alle lidstaten moeten worden toegelaten. De bevoegde toezichthoudende autoriteit zal het EDPB een ontwerp verstrekken op het moment dat zij van mening is dat de criteria door het EDPB zullen worden goedgekeurd.

37. De keuze waar een aanvraag voor goedkeuring van criteria wordt ingediend, wordt bepaald door de plaats van het hoofdkantoor van de eigenaren van een certificeringsregeling of de certificeringsorganen.

38. Indien een certificeringsorgaan een aanvraag indient, gebeurt dat normaal binnen de aanvraagprocedure voor accreditatie of heeft de accreditatie al plaatsgevonden door de bevoegde toezichthoudende autoriteit of de nationale accreditatie-instantie van de betreffende lidstaat. Wanneer het certificeringsorgaan al geaccrediteerd is voor een AVG-certificeringsmechanisme, kan dit bijdragen aan de stroomlijning van de goedkeuringsprocedure.

4.2.2 Criteria voor een Europees gegevensbeschermingszegel

39. Het EDPB zal de beoordelingsprocedure coördineren en de criteria voor een Europees gegevensbeschermingszegel goedkeuren, zoals vereist. Bij de beoordeling wordt onder andere gekeken naar: het toepassingsgebied van de criteria en de geschiktheid ervan om als gemeenschappelijk certificaat te dienen. Indien de criteria door het EDPB zijn goedgekeurd, moet de bevoegde toezichthoudende autoriteit waaronder het Europese hoofdkantoor van het certificeringsorgaan valt, klachten over het betreffende mechanisme afhandelen en andere toezichthoudende autoriteiten hiervan op de hoogte stellen. Deze toezichthoudende autoriteit is eveneens bevoegd om maatregelen ten aanzien van het certificeringsorgaan te nemen. Naargelang van het geval zal de bevoegde toezichthoudende autoriteit de andere toezichthoudende autoriteiten en het EDPB niet op de hoogte stellen.

40. Certificeringscriteria die tot een gemeenschappelijk certificaat moeten leiden, krijgen te maken met EU-brede aanvragen en moeten een specifiek mechanisme bieden om hiermee om te gaan. Europese certificeringsmechanismen moeten bedoeld zijn voor gebruik in alle lidstaten. Overeenkomstig artikel 42, lid 5, moeten het mechanisme voor een Europees gegevensbeschermingszegel en de bijbehorende criteria aanpasbaar zijn, zodat waar nodig rekening kan worden gehouden met nationale bedrijfstakspecifieke voorschriften,

bijvoorbeeld voor gegevensverwerking in scholen, en moet een EU-brede toepasbaarheid zijn voorzien.

41. Voorbeeld: een internationale school die onderwijs biedt aan betrokkenen in de Unie, is gevestigd in lidstaat "A". Deze school wil zijn online aanvraagprocedure met een EU-brede certificeringsregeling certificeren om een Europees gegevensbeschermingszegel te verkrijgen. De school wil een aanvraag indienen voor de certificering van verwerkingen door een certificeringsorgaan dat gevestigd is in lidstaat "B", op basis van een Europees gegevensbeschermingszegel. De criteria voor het zegel die zijn opgesteld en zijn vastgelegd in het betreffende mechanisme, moeten rekening kunnen houden met de voorschriften voor scholen die van toepassing zijn in lidstaat "A". Op grond van de criteria moet de online aanvraagprocedure van de school ook informatie verstrekken over en rekening houden met de toepasselijke voorschriften inzake gegevensbescherming van de lidstaat, die kunnen verschillen van die van andere lidstaten. Een voorbeeld hiervan zijn de persoonsgegevens die voor de aanvraag moeten worden ingediend, bijvoorbeeld cijfers van de kleuterschool of testresultaten, afwijkende bewaringstermijnen, verzameling of verwerking van financiële of biometrische gegevens, andere verwerkingsbeperkingen.

- Strenge criteria voor de goedkeuring van een mechanisme voor een Europees gegevensbeschermingszegel omvatten:
  - door het Comité goedgekeurde criteria;
  - toepasbaarheid in verschillende rechtsgebieden, waar nodig rekening houdend met nationale wettelijke eisen en bedrijfstakspecifieke voorschriften;
  -
- geharmoniseerde criteria, die aanpasbaar zijn om rekening te kunnen houden met nationale eisen;
  - een beschrijving van het certificeringsmechanisme, met een specificatie van:
  - de certificeringsovereenkomst, waarin pan-Europese eisen worden erkend;
  - procedures om oplossingen voor nationale verschillen te bieden en ervoor te zorgen dat met het zegel de overeenstemming van de AVG kan worden aangetoond; en
  - de taal van de verslagen voor alle betrokken toezichthoudende autoriteiten.

42. De bijlage bevat bovendien advies over de criteria voor het Europees gegevensbeschermingszegel.

4.2.3 De rol van accreditatie

43. Zoals opgemerkt in paragraaf 4.2.1 kunnen certificeringsorganen, als criteria geschikt zijn bevonden om tot een gemeenschappelijk certificaat te leiden, en als zodanig zijn

goedgekeurd door het Comité overeenkomstig artikel 42, lid 5, worden geaccrediteerd om certificeringen volgens deze criteria af te geven op Unieniveau.

44. Regelingen die uitsluitend bedoeld zijn om in bepaalde lidstaten te worden aangeboden, kunnen niet in aanmerking komen voor EU-zegels. Voor accreditatie voor een Europees gegevensbeschermingszegel is accreditatie nodig in de lidstaat waar het hoofdkantoor is gevestigd van het certificeringsorgaan dat de regeling wil gaan uitvoeren, dat wil zeggen dat verantwoordelijk is voor de afgifte van certificeringen en het beheer van de certificeringsactiviteiten van haar entiteiten en dochterondernemingen in andere lidstaten. Indien andere vestigingen of kantoren zelfstandig certificeringen beheren en uitvoeren, moeten deze vestigingen of kantoren afzonderlijk geaccrediteerd worden in de lidstaat van vestiging. Accreditatie is met andere woorden alleen noodzakelijk in de lidstaat van vestiging van de hoofdkantoren van het certificeringsorgaan als alleen de hoofdkantoren de certificeringen afgeven. Indien daarentegen ook andere vestigingen van het certificeringsorgaan certificeringen afgeven, moeten deze vestigingen eveneens zijn geaccrediteerd.

45. Indien een certificeringsorgaan dus niet is geaccrediteerd voor certificering volgens het Europees gegevensbeschermingszegel, kunnen de door de EDPB goedgekeurde criteria niet worden gebruikt en kan er geen zegel worden aangeboden.

5 ONTWIKKELING VAN CERTIFICERINGSCRITERIA

46. De AVG heeft het kader voor de ontwikkeling van certificeringscriteria vastgesteld. Terwijl fundamentele vereisten voor de certificeringsprocedure aan de orde komen in de artikelen 42 en 43, die eveneens belangrijke criteria voor certificeringsprocedures bevatten, is de grondslag voor certificeringscriteria te vinden in de beginselen en regels van de AVG, die eraan bijdragen dat de criteria worden nageleefd.

47. De ontwikkeling van certificeringscriteria moet zich richten op de verifieerbaarheid, het belang en de geschiktheid van certificeringscriteria om naleving van de verordening aan te tonen. Certificeringscriteria moeten zo worden opgesteld dat zij duidelijk en begrijpelijk zijn en praktisch kunnen worden toegepast.

48. Bij het opstellen van certificeringscriteria moeten de volgende aspecten van overeenstemming ter ondersteuning van onder andere de beoordeling van de verwerkingen, indien van toepassing, in aanmerking worden genomen:

- de rechtmatigheid van de verwerking overeenkomstig artikel 6;
- de beginselen van gegevensverwerking overeenkomstig artikel 5;
- de rechten van de betrokkenen overeenkomstig de artikelen 12 tot en met 23;
- de verplichting om inbreuken te melden overeenkomstig artikel 33;
- de verplichting van gegevensbescherming door ontwerp en door standaardinstellingen, overeenkomstig artikel 25;

- of, indien van toepassing, een gegevensbeschermingseffectbeoordeling overeenkomstig artikel 35, lid 7, onder d), is uitgevoerd; en
- de technische en organisatorische maatregelen die getroffen zijn overeenkomstig artikel 32.

49. De mate waarin deze aspecten in de criteria terugkomen, kan variëren afhankelijk van het toepassingsgebied van de certificering, waaronder de aard van de verwerking(en) en het gebied (bv. gezondheid) kunnen vallen.

5.1 Welke certificeringen zijn op grond van de AVG mogelijk?

50. Het EDPB is van mening dat de AVG ruime mogelijkheden biedt voor certificering volgens de AVG, mits dit bedoeld is om te helpen aantonen dat verwerkingsverantwoordelijken en verwerkers bij verwerkingen in overeenstemming met deze verordening handelen (artikel 42, lid 1).

51. Bij de beoordeling van een verwerking moet, indien van toepassing, rekening worden gehouden met de volgende drie belangrijke elementen:

    1. persoonsgegevens (materieel toepassingsgebied van de AVG);
    2. technische systemen – de infrastructuur, zoals hardware en software, die wordt gebruikt om de persoonsgegevens te verwerken; en
    3. processen en procedures die verband houden met de verwerking(en).

52. Elk element dat bij de verwerkingen wordt gebruikt, moet aan de hand van de vastgestelde criteria worden beoordeeld. Er zijn ten minste vier verschillende belangrijke factoren die van invloed kunnen zijn: 1) de organisatie en de rechtsvorm van de verwerkingsverantwoordelijke of verwerker; 2) de afdeling, de omgeving en de mensen die bij de verwerking(en) zijn betrokken; 3) de technische beschrijving van de te beoordelen elementen; 4) de IT-infrastructuur die als basis dient voor de verwerking, waaronder besturingssystemen, virtuele systemen, databanken, authenticatie- en autorisatiesystemen, routers en firewalls, opslagsystemen, communicatie-infrastructuur of internettoegang en aanverwante technische voorzieningen.

53. Alle drie belangrijke elementen zijn van belang voor het ontwerp van certificeringsprocedures en -criteria. Afhankelijk van het voorwerp van certificering, kan de mate waarin deze elementen in aanmerking worden genomen, variëren. Zo kunnen sommige elementen in bepaalde gevallen buiten beschouwing worden gelaten als zij niet relevant worden geacht voor het voorwerp van certificering.

54. In aanvullende richtsnoeren in de AVG wordt verder beschreven welke certificeringen op grond van deze verordening mogelijk zijn. Uit artikel 42, lid 7, volgt dat op grond van de AVG alleen certificeringen kunnen worden afgegeven aan verwerkingsverantwoordelijken en verwerkers, waarmee bijvoorbeeld de certificering van functionarissen voor gegevensbescherming wordt uitgesloten. In artikel 43, lid 1, onder b), wordt verwezen naar

ISO 17065, de norm voor accreditatie van certificeringsorganen die de conformiteit beoordelen van producten, processen en diensten. Een verwerking of een reeks verwerkingen kan de hoedanigheid krijgen van een product of dienst in de zin van ISO 17065, waarvoor certificering nodig kan zijn. Zo bestaat de verwerking van werknemersgegevens voor salarisbetaling of het beheer van verlofdagen uit een reeks verwerkingen in de zin van de AVG, die de hoedanigheid kan krijgen van een product, proces of dienst in de zin van ISO.

55. Daarom is het EDPB van oordeel dat het toepassingsgebied van de certificering volgens de AVG gericht is op verwerkingen of reeksen verwerkingen. Daartoe kunnen bestuursprocessen in de zin van organisatorische maatregelen behoren, die integrale onderdelen van een verwerking zijn (bv. het bestuursproces dat is opgesteld voor de afhandeling van klachten als onderdeel van de verwerking van werknemersgegevens voor salarisbetaling).

56. Om te beoordelen of de verwerking in overeenstemming is met de certificeringscriteria, is een use case nodig. Zo hangt de overeenstemming van het gebruik van technische infrastructuur binnen een verwerking samen met de categorieën gegevens waarvoor deze infrastructuur is ontworpen. Organisatorische maatregelen hangen samen met de categorieën en de hoeveelheid gegevens en de technische infrastructuur die voor de verwerking wordt gebruikt, rekening houdend met de aard, omvang, inhoud en doelen van de verwerking en de risico's voor de rechten en vrijheden van de betrokkenen.

57. Bovendien mag niet uit het oog worden verloren dat IT-toepassingen sterk uiteen kunnen lopen, ook als zij dezelfde verwerkingsdoeleinden dienen. Hiermee moet rekening worden gehouden bij het vaststellen van het toepassingsgebied van de certificeringsmechanismen en het opstellen van de certificeringscriteria, dat wil zeggen dat binnen het toepassingsgebied van certificering en criteria ruimte moet worden gelaten voor anders ontworpen IT-toepassingen.

5.2 Het vaststellen van het voorwerp van certificering

58. Het toepassingsgebied van een certificeringsmechanisme moet los worden gezien van het voorwerp – ook het onderwerp van beoordeling genoemd – in individuele certificeringsprojecten in overeenstemming met een certificeringsmechanisme. Voor een certificeringsmechanisme kan het toepassingsgebied algemeen of in verband met een bepaald type gebied van verwerkingen worden vastgesteld. Zo kunnen op voorhand de voorwerpen van certificering worden bepaald die binnen het toepassingsgebied van het certificeringsmechanisme vallen (bv. veilige opslag en bescherming van persoonsgegevens in een digitale kluis). Er kan alleen op elk moment een betrouwbare, zinvolle beoordeling van de conformiteit worden gemaakt als het individuele voorwerp van een certificeringsproject nauwkeurig wordt beschreven. Er moet duidelijk worden beschreven welke verwerkingen tot het voorwerp van certificering behoren en vervolgens welke belangrijke elementen, dat wil zeggen gegevens, processen en technische infrastructuur, zullen worden beoordeeld en welke niet. Daarbij moet ook altijd de aansluiting met andere processen in aanmerking worden genomen en worden beschreven. Immers, wat onbekend is kan niet worden beoordeeld en dus ook niet worden gecertificeerd. In ieder geval moet het individuele

voorwerp van certificering aansluiten bij de boodschap of de gemaakte claim op/door de certificering en mag het de gebruiker, klant of consument niet misleiden.

59. [Voorbeeld 1]

Een bank biedt haar klanten een website aan waarmee zij online kunnen bankieren. Binnen deze dienst is het mogelijk geld over te maken, aandelen te kopen, opdrachten voor periodieke overboekingen in te stellen en de rekening te beheren. De bank wil de volgende onderdelen laten certificeren in overeenstemming met een certificeringsmechanisme voor gegevensbescherming met een algemeen toepassingsgebied gebaseerd op algemene criteria:

a) Veilige log-in

Een veilige log-in speelt een belangrijke rol bij de beveiliging van de betrokken persoonsgegevens en is daarom een verwerking die begrijpelijk is voor de eindgebruiker en relevant vanuit een oogpunt van gegevensbescherming. Deze verwerking is daarom noodzakelijk om veilig te kunnen inloggen en kan bijgevolg een zinvol onderwerp van beoordeling vormen, als in het certificaat duidelijk wordt vermeld dat alleen de verwerking van de log-in is gecertificeerd.

b) Front-end van de website

Hoewel de front-end van de website vanuit een oogpunt van gegevensbescherming belangrijk kan zijn, is dat voor de eindgebruiker niet begrijpelijk. Daarom kan het niet als een zinvol onderwerp van beoordeling worden beschouwd. Bovendien is het voor de gebruiker niet duidelijk welke diensten op de website, en dus welke verwerkingen, onder de certificering vallen.

c) Online bankieren

De front-end en back-end van de website samen vormen verwerkingen binnen de onlinebankierendienst die zinvol kunnen zijn voor de gebruiker. In dat verband moeten zij beide deel uitmaken van het onderwerp van beoordeling. Verwerkingen die niet direct samenhangen met de levering van de onlinebankierendienst, zoals verwerkingen met als doel witwassen te voorkomen, kunnen juist van het onderwerp van beoordeling worden uitgesloten.

De onlinebankierendiensten die de bank via haar website aanbiedt, kunnen echter ook andere diensten omvatten, waarvoor weer aparte verwerkingen nodig zijn. In dat verband kunnen andere diensten bijvoorbeeld het aanbieden van een verzekeringsproduct zijn. Aangezien deze aanvullende dienst niet direct verband houdt met het doel van onlinebankierendiensten, kan het van het onderwerp van beoordeling worden uitgesloten. Als deze aanvullende dienst (verzekering) van het onderwerp van beoordeling wordt uitgesloten, maken de interfaces voor deze in de website verwerkte dienst wel deel uit van het onderwerp van beoordeling, moeten ze derhalve worden beschreven, zodat een duidelijk onderscheid tussen de diensten kan worden gemaakt. Deze beschrijving is nodig om eventuele gegevensstromen tussen de beide diensten te kunnen vaststellen en beoordelen.

60. [Voorbeeld 2]

Een bank biedt haar klanten een dienst aan waarmee zij de informatie van verschillende rekeningen en creditcards van verschillende banken kunnen koppelen (samenvoeging van rekeningen). De bank wil deze dienst op grond van de AVG laten certificeren. De bevoegde toezichthoudende autoriteit heeft een specifieke reeks certificeringscriteria voor dit type activiteit goedgekeurd. Het toepassingsgebied van het certificeringsmechanisme betreft alleen de volgende aspecten van overeenstemming:

- gebruikersauthenticatie; en
- aanvaardbare methoden om samen te voegen gegevens van andere banken/diensten te verkrijgen.

Aangezien het onderwerp van beoordeling al bepaald wordt door het toepassingsgebied van dit certificeringsmechanisme, kan het onderwerp van beoordeling in het licht van dat toepassingsgebied niet zinvol worden afgebakend en is het niet mogelijk alleen specifieke onderdelen of een afzonderlijke verwerkingsactiviteit te certificeren. In deze situatie moet een onderwerp van beoordeling overeenkomen met een specifiek toepassingsgebied.

5.3 Evaluatiemethoden en beoordelingsmethodologie

61. Voor een conformiteitsbeoordeling die de overeenstemming van verwerkingen moet helpen aantonen, moeten eerst de evaluatiemethoden en de beoordelingsmethodologie worden vastgesteld en bepaald. Het maakt uit of voor de beoordeling gebruikte informatie uitsluitend verkregen is uit documenten (wat op zich onvoldoende is) of ter plaatse en via directe of indirecte toegang actief is verzameld. De wijze waarop informatie wordt verzameld, heeft gevolgen voor de betekenis van certificering en moet daarom worden vastgesteld en beschreven.

    Procedures voor de afgifte en de periodieke toetsing van certificeringen moeten specificaties bevatten voor de vaststelling van een passend evaluatieniveau (in diepte en detail) om aan de certificeringscriteria te voldoen en moeten het volgende omvatten:

    - informatie over en specificaties van de toegepaste beoordelingsmethoden en bevindingen die zijn gedaan, bijvoorbeeld tijdens onderzoeken ter plaatse of aan de hand van documenten;
    - evaluatiemethoden voor verwerkingen (gegevens, systemen, processen) en het verwerkingsdoel;
    - beschrijvingen van de categorieën gegevens, van de vereiste bescherming en of verwerkers of derden zijn betrokken;
    - beschrijvingen van functies en van het bestaan van een toegangscontrolemechanisme voor mensen met bepaalde functies en verantwoordelijkheden.

62. De diepgang van de evaluatie is van invloed op de betekenis en de waarde van de certificering. Door wegens pragmatische redenen of om de kosten te verlagen de diepgang uit de evaluatie te halen, zal de certificering voor gegevensbescherming aan belang inboeten. Anderzijds kunnen beslissingen over de gedetailleerdheid van een evaluatie de financiële

mogelijkheden van de aanvrager en vaak ook de mogelijkheden van beoordelaars en auditoren te boven gaan. Om de overeenstemming aan te tonen is het niet altijd noodzakelijk een zeer gedetailleerde analyse van de gebruikte IT-systemen te maken.

5.4 Documentatie van de beoordelingen

63. Certificeringen moeten grondig en uitgebreid worden gedocumenteerd. Bij een gebrek aan documentatie kan geen goede beoordeling plaatsvinden. Documentatie is bij certificering essentieel voor de transparantie van het evaluatieproces van het certificeringsmechanisme. Aan de hand van documentatie kan verantwoording worden afgelegd ten aanzien van de wettelijke eisen. Certificeringsmechanismen moeten een gestandaardiseerde methodologie voor de documentatie omvatten. Tijdens een evaluatie kan de certificeringsdocumentatie dan worden vergeleken met de daadwerkelijke situatie ter plaatse en met de certificeringscriteria.

64. Uitgebreide documentatie over wat is gecertificeerd en welke methodologie is gebruikt, is bevorderlijk voor de transparantie. Overeenkomstig artikel 43, lid 2, onder c), moeten in certificeringsmechanismen procedures worden vastgesteld die de toetsing van certificeringen mogelijk maken. Om de toezichthoudende autoriteit in de gelegenheid te stellen te beoordelen of en in hoeverre de certificering in formele onderzoeken kan worden erkend, kan uitvoerige documentatie het middel bij uitstek zijn. Voor tijdens evaluaties opgestelde documentatie zijn daarom drie aspecten van belang:

    - de consistentie en samenhang van de gehanteerde evaluatiemethoden;
    - de evaluatiemethoden die erop zijn gericht om aan te tonen dat het voorwerp van certificering en de certificeringscriteria met elkaar en de verordening overeenstemmen; en
    - de evaluatieresultaten, die moeten zijn gevalideerd door een onafhankelijk en onpartijdig certificeringsorgaan.

5.5 Documentatie van de resultaten

65. Overweging 100 beschrijft de doelstellingen die worden nagestreefd met de invoering van certificatie.

"Teneinde de transparantie en naleving van deze verordening te versterken, dient het instellen van certificeringsmechanismen en gegevensbeschermingszegels en -merktekens te worden bevorderd, zodat betrokkenen snel het gegevensbeschermingsniveau van producten en diensten ter zake kunnen beoordelen."

66. Om de transparantie te verbeteren zijn een goede documentatie en communicatie van belang. Certificeringsorganen die certificeringsmechanismen, zegels of merktekens gebruiken die zijn gericht op de betrokkenen (in hun hoedanigheid als consument of klant), moeten gemakkelijk toegankelijke, begrijpelijke en zinvolle informatie over de gecertificeerde

verwerking(en) verstrekken. Deze openbare informatie moet ten minste het volgende omvatten:

- de beschrijving van het onderwerp van beoordeling;
- een verwijzing naar het goedgekeurde criterium dat op het specifieke onderwerp van beoordeling is toegepast;
- de methodologie voor de evaluatie van het criterium (evaluatie ter plaatse, documentatie enz.); en
- de geldigheidsduur van het certificaat; en
- de mogelijkheid voor toezichthoudende autoriteiten en het publiek om resultaten te vergelijken.

6 RICHTSNOEREN VOOR HET VASTSTELLEN VAN CERTIFICERINGSCRITERIA

67. Certificeringscriteria maken integraal deel uit van een certificeringsmechanisme. In de certificeringsprocedure wordt bepaald hoe, door wie, in hoeverre en hoe specifiek de beoordeling moet plaatsvinden in individuele certificeringsprojecten ten aanzien van een specifiek voorwerp of onderwerp van beoordeling. De certificeringscriteria omvatten de nominale vereisten op grond waarvan de in het onderwerp van beoordeling vastgestelde verwerking wordt beoordeeld. Deze richtsnoeren voor het vaststellen van certificeringscriteria geven algemene aanwijzingen die de beoordeling van certificeringscriteria met het oog op goedkeuring, vergemakkelijken.

    - Bij het goedkeuren of vaststellen van certificeringscriteria moeten de volgende algemene overwegingen in aanmerking worden genomen. Certificeringscriteria moeten:
    - uniform en verifieerbaar zijn;
    - controleerbaar zijn om de evaluatie van verwerkingen op grond van de AVG te vergemakkelijken, door in het bijzonder de doelstellingen en de richtsnoeren voor de uitvoering van deze doelstellingen te specificeren;
    - relevant zijn voor de beoogde doelgroep (bv. B2B en B2C);
    - rekening houden met en, indien nodig, aansluiten op andere normen (zoals ISO-normen en nationale normen); en
    - flexibel en schaalbaar zijn voor toepassing op organisaties van verschillende typen en grootten, waaronder kleine, middelgrote en micro-ondernemingen overeenkomstig artikel 42, lid 1, en de op risico gebaseerde benadering overeenkomstig overweging 77.

68. Een kleine lokale onderneming, zoals een winkelier, zal doorgaans minder complexe verwerkingen uitvoeren dan een grote multinational. De voorschriften inzake de rechtmatigheid van de verwerkingen zijn weliswaar dezelfde, maar er moet wel rekening worden gehouden met het toepassingsgebied van de gegevensverwerking en de complexiteit ervan. Hieruit volgt dat het noodzakelijk is dat certificeringsmechanismen en de bijbehorende criteria schaalbaar zijn ten aanzien van de betreffende verwerkingsactiviteit.

6.1 Bestaande normen

69. Certificeringsorganen moeten overwegen hoe in specifieke criteria rekening wordt gehouden met bestaande relevante instrumenten, zoals gedragscodes, technische normen of nationale regelgevings- en wetgevingsinitiatieven. In een ideale situatie sluiten criteria aan op bestaande normen, waardoor een verwerkingsverantwoordelijke of verwerker aan zijn verplichtingen uit hoofde van de AVG kan voldoen. Industrienormen richten zich echter veelal op de bescherming en de veiligheid van de organisatie ten aanzien van bedreigingen, terwijl de AVG gericht is op de bescherming van grondrechten van natuurlijke personen. Met dit verschil moet bij het opstellen van criteria of het goedkeuren van criteria of certificeringsmechanismen op basis van industrienormen rekening worden gehouden.

6.2 Vaststellen van criteria

70. Certificeringscriteria moeten overeenstemmen met de certificeringsverklaring (boodschap of claim) van een certificeringsmechanisme of -regeling en moeten voldoen aan de verwachtingen die zij wekken. De naam van een certificeringsmechanisme kan al een aanwijzing inhouden voor het toepassingsgebied, wat gevolgen heeft voor de vaststelling van criteria.

71. [Voorbeeld 3]

    Voor een mechanisme met de naam "MerktekenPrivacyGezondheid" zou het toepassingsgebied moeten worden beperkt tot de gezondheidssector. Op grond van de zegelnaam wordt de verwachting gewekt dat vereisten voor gegevensbescherming zijn getoetst in relatie tot gegevens over gezondheid. Daarom moeten de criteria van dit mechanisme geschikt zijn om vereisten voor gegevensbescherming binnen deze sector te beoordelen.

72. [Voorbeeld 4]

    Voor een mechanisme dat verband houdt met de certificering van verwerkingen waaronder bestuurssystemen binnen de gegevensverwerking vallen, moeten criteria worden vastgesteld waarmee bestuursprocessen en de bijbehorende technische en organisatorische maatregelen kunnen worden erkend en beoordeeld.

73. [Voorbeeld 5]

    Voor de criteria voor een mechanisme dat verband houdt met cloudoplossingen, moeten de speciale technische eisen die nodig zijn voor het gebruik van clouddiensten, in aanmerking

worden genomen. Bijvoorbeeld, als servers zich buiten de EU bevinden, moet in de criteria rekening worden gehouden met de voorwaarden uit hoofdstuk V van de AVG ten aanzien van gegevensdoorgifte naar derde landen.

74. Criteria die zijn opgesteld voor verschillende onderwerpen van beoordeling in verschillende sectoren en/of lidstaten, moeten aan het volgende voldoen: ze moeten de toepassing op verschillende situaties mogelijk maken; ze moeten het mogelijk maken passende maatregelen vast te stellen voor kleine, middelgrote of grote verwerkingen en ze moeten de risico's van verschillende waarschijnlijkheid en ernst weerspiegelen voor de rechten en vrijheden van natuurlijke personen overeenkomstig de AVG. De certificeringsprocedures (bv. voor documentatie, tests of evaluatiemethode en diepte) die de criteria aanvullen, moeten dan ook aan deze behoeften voldoen en voor regels zorgen of de mogelijkheden bieden om bijvoorbeeld de betreffende criteria in individuele certificeringsprojecten toe te passen. Criteria moeten een beoordeling mogelijk maken of voldoende waarborgen zijn gegeven om passende technische en organisatorische maatregelen in te voeren.

6.3 Levensduur van certificeringscriteria

75. Hoewel certificeringscriteria langere tijd betrouwbaar moeten zijn, is het niet nodig dat zij onbeperkt houdbaar zijn. Zo moeten zij worden herzien als:

- het rechtskader is veranderd;
- voorwaarden en bepalingen zijn uitgelegd in arresten van het Hof van Justitie van de Europese Unie; of
- de actuele stand van de techniek is veranderd.

Namens het Europees Comité voor gegevensbescherming

De voorzitter

(Andrea Jelinek)

BIJLAGE 1: TAKEN EN BEVOEGDHEDEN VAN TOEZICHTHOUDENDE AUTORITEITEN IN VERBAND MET CERTIFICERING OVEREENKOMSTIG DE AVG

	Bepalingen	Vereisten
Taken	Artikel 43, lid 6	Vereist dat de in artikel 42, lid 5, bedoelde criteria door de toezichthoudende autoriteit in een eenvoudig toegankelijke vorm openbaar worden gemaakt en aan het Comité worden meegedeeld.
	Artikel 57, lid 1, onder n)	Vereist dat de toezichthoudende autoriteit de criteria voor certificering uit hoofde van artikel 42, lid 5, goedkeurt.
	Artikel 57, lid 1, onder o)	Bepaalt dat waar van toepassing (d.w.z. waar zij een certificering afgeeft), zij een periodieke toetsing verricht van de overeenkomstig artikel 42, lid 7, afgegeven certificeringen.
	Artikel 64, lid 1, onder c)	Vereist dat de toezichthoudende autoriteit het Comité het ontwerpbesluit meedeelt indien het beoogt de criteria voor certificering als bedoeld in artikel 42, lid 5, goed te keuren.
Bevoegdheden	Artikel 58, lid 1, onder c)	Bepaalt dat de toezichthoudende autoriteit bevoegd is een toetsing te verrichten van de overeenkomstig artikel 42, lid 7, afgegeven certificeringen.
	Artikel 58, lid 2, onder h)	Bepaalt dat de toezichthoudende autoriteit bevoegd is een certificering in te trekken of het certificeringsorgaan te gelasten een afgegeven certificering in te trekken, of het certificeringsorgaan te gelasten geen certificering af te geven.
	Artikel 58, lid 3, onder e)	Bepaalt dat de toezichthoudende autoriteit bevoegd is certificeringsorganen te accrediteren.
	Artikel 58, lid 3, onder f)	Bepaalt dat de toezichthoudende autoriteit bevoegd is certificeringen af te geven en certificeringscriteria goed te keuren.
	Artikel 58, lid 3, onder e)	Bepaalt dat de toezichthoudende autoriteit bevoegd is certificeringsorganen te accrediteren.
	Artikel 58, lid 3, onder f)	Bepaalt dat de toezichthoudende autoriteit bevoegd is certificeringen af te geven en certificeringscriteria goed te keuren.

BIJLAGE 2

1 INLEIDING

Bijlage 2 bevat richtsnoeren voor het herzien en beoordelen van certificeringscriteria overeenkomstig artikel 42, lid 5. Hierin worden onderwerpen aan de orde gesteld die een toezichthoudende autoriteit voor gegevensbescherming en het comité in overweging zullen nemen en zullen toepassen met het oog op de goedkeuring van de certificeringscriteria van een certificeringsmechanisme. De vragen moeten in overweging worden genomen door certificeringsorganen en eigenaren van een certificeringsregeling die criteria willen opstellen en ter goedkeuring willen indienen. De lijst is niet volledig, maar bevat enkel de punten die op zijn minst in aanmerking moeten worden genomen. Niet alle vragen zullen ter zake doen. Ze moeten echter wel in overweging worden genomen bij het opstellen van criteria en er kan een bepaalde redenering nodig zijn om uit te leggen waarom bepaalde criteria bepaalde aspecten niet dekken. Sommige vragen worden herhaald en vanuit verschillende gezichtspunten gesteld. Deze richtsnoeren moeten in overweging worden genomen overeenkomstig de wettelijke bepalingen van de AVG en, indien van toepassing, van nationale wetgeving.

2 TOEPASSINGSGEBIED VAN HET CERTIFICERINGSMECHANISME EN ONDERWERP VAN BEOORDELING

a. Is het toepassingsgebied van het certificeringsmechanisme (waarvoor de criteria voor gegevensbescherming moeten worden gebruikt) duidelijk beschreven?

b. Is het toepassingsgebied van het certificeringsmechanisme relevant voor de beoogde doelgroep en niet misleidend?

- *Voorbeeld: Het "zegel van een betrouwbare onderneming" suggereert dat de verwerkingsactiviteiten van een gehele onderneming zijn gecontroleerd, hoewel alleen bepaalde verwerkingen, zoals het online betalingsproces, daadwerkelijk zijn gecertificeerd. Het toepassingsgebied is in dat geval misleidend.*

c. Omvat het toepassingsgebied van het certificeringsmechanisme alle relevante aspecten van de verwerkingen?

- *Voorbeeld: Een "privacymerkteken voor de gezondheidssector" moet alle beoordelingsgegevens betreffende gezondheid omvatten om aan de vereisten van artikel 9 te kunnen voldoen.*

d. Staat het toepassingsgebied van het certificeringsmechanisme een zinvolle certificering van gegevensbescherming toe rekening houdend met de aard, de inhoud en het risico van de bijbehorende verwerkingen?

- *Voorbeeld: Indien het toepassingsgebied van het certificeringsmechanisme zich uitsluitend richt op bepaalde aspecten van verwerkingen, zoals de verzameling van gegevens, maar niet op de rest van de verwerkingen, zoals verwerkingen met als doel het opstellen van advertentieprofielen of het beheren van rechten van betrokkenen, zou dat voor betrokkenen niet zinvol zijn.*

e. Omvat het toepassingsgebied van het certificeringsmechanisme de verwerking van persoonsgegevens in het betreffende land van toepassing of betreft het grensoverschrijdende verwerking en/of gegevensdoorgiften?

f. Beschrijven de certificeringscriteria in voldoende mate hoe het onderwerp van beoordeling moet worden vastgesteld?

- *Voorbeeld: Een "privacyzegel" voor een algemeen toepassingsgebied waarvoor alleen "een specificatie van de verwerking die moet worden gecertificeerd" is vereist, kan onvoldoende houvast bieden voor het vaststellen en beschrijven van een onderwerp van beoordeling.*
- *Voorbeeld: Een (specifiek) toepassingsgebied, "Het kluiszegel voor privacy", dat zich richt op veilige opslag, moet een gedetailleerde beschrijving geven van de vereisten om aan de criteria voor dit toepassingsgebied te voldoen, bijvoorbeeld de definitie van kluis, systeemvereisten, verplichte technische en organisatorische maatregelen. In dat geval kan het toepassingsgebied het onderwerp van beoordeling duidelijk vaststellen.*

(1) Moeten op grond van de criteria voor het onderwerp van beoordeling alle relevante verwerkingen worden vastgesteld, gegevensstromen worden weergegeven en het toepassingsgebied van de onderwerpen van beoordeling worden vastgesteld?

- *Voorbeeld: Een certificeringsmechanisme maakt de certificering van verwerkingen van verwerkingsverantwoordelijken op grond van de AVG mogelijk, zonder dat een verdere specificatie van het toepassingsgebied (algemeen toepassingsgebied) nodig is. Op grond van de criteria van het mechanisme moet de aanvragende verwerkingsverantwoordelijke de gegevenstypen, systemen en processen van de beoogde verwerking (onderwerp van beoordeling) vaststellen.*

(2) Moet de aanvrager op grond van de criteria het begin en het einde van de verwerking die wordt beoordeeld, toelichten? Moet het onderwerp van beoordeling op grond van de criteria interfaces omvatten, indien onderling afhankelijke verwerkingen geen deel uitmaken van het onderwerp van beoordeling? En wordt dit naar tevredenheid onderbouwd?

- *Voorbeeld: Een onderwerp van beoordeling met een toereikende beschrijving van de verwerking van een webdienst, bijvoorbeeld waarbij sprake is van de registratie van gebruikers, de verlening van diensten, facturering, de vastlegging van IP-adressen en gebruikers- en derdeninterfaces, maar niet van serverhosting (maar wel inclusief verwerkingsovereenkomsten en overeenkomsten voor technische en organisatorische maatregelen).*

g. Waarborgen de criteria dat de (individuele) onderwerpen van beoordeling begrijpelijk zijn voor het publiek, waaronder eventuele betrokkenen?

3 ALGEMENE VOORSCHRIFTEN

a. Worden alle relevante termen in de lijst van criteria (d.w.z. de volledige certificeringscriteria) gedefinieerd, verklaard en beschreven?

b. Zijn alle normatieve verwijzingen geïdentificeerd?

c. Definiëren de criteria verantwoordelijkheden ten aanzien van gegevensbescherming, procedures en verwerkingen onder het toepassingsgebied van het certificeringsmechanisme?

4 VERWERKING, ARTIKEL 42, LID 1

Komen ten aanzien van het toepassingsgebied van het certificeringsmechanisme (algemeen of specifiek) alle relevante onderdelen van de verwerkingen (gegevens, systemen en processen) in de criteria aan de orde?

a. Moet op grond van de criteria de geldige wettelijke basis voor verwerking ten aanzien van het onderwerp van beoordeling worden geïdentificeerd?

b. Worden in de criteria ten aanzien van het onderwerp van beoordeling de relevante cycli van de verwerking en de volledige levenscyclus van gegevens, inclusief het wissen en anonimiseren, erkend?

c. Wordt in de criteria ten aanzien van het onderwerp van beoordeling gegevensoverdraagbaarheid vereist?

d. Bieden de criteria ten aanzien van het onderwerp van beoordeling de mogelijkheid om speciale typen verwerkingen, bijvoorbeeld geautomatiseerde besluitvorming, profilering, te identificeren en in aanmerking te nemen?

e. Bieden de criteria ten aanzien van het onderwerp van beoordeling de mogelijkheid om bijzondere categorieën gegevens te identificeren?

f. Bieden de criteria de mogelijkheid om het risico van individuele verwerkingen en de vereiste bescherming van rechten en vrijheden van betrokkenen te beoordelen en vereisen zij dit?

g. Bieden de criteria de mogelijkheid om naar behoren rekening te houden met de risico's voor de rechten en vrijheden van natuurlijke personen en vereisen zij dit?

…

5 RECHTMATIGHEID VAN DE VERWERKING

a. Vereisen de criteria dat wordt gecontroleerd of individuele verwerkingen wat betreft het doel en de noodzaak ervan rechtmatig zijn?

b. Vereisen de criteria dat gecontroleerd wordt of aan alle vereisten voor een rechtsgrondslag voor individuele verwerkingen wordt voldaan?

6 BEGINSELEN, ARTIKEL 5

a. Komen de criteria tegemoet aan alle beginselen van gegevensbescherming overeenkomstig artikel 5?

b. Moet er op grond van de criteria worden aangetoond dat voor het individuele onderwerp van beoordeling een minimale gegevensverwerking is toegepast?

…

7 ALGEMENE VERPLICHTINGEN VAN VERWERKINGSVERANTWOORDELIJKEN EN VERWERKERS

a. Wordt op grond van de criteria bewijs verlangd voor contractuele overeenkomsten tussen verwerkers en verwerkingsverantwoordelijken?

b. Moeten overeenkomsten tussen verwerkers en verwerkingsverantwoordelijken worden beoordeeld?

c. Weerspiegelen de criteria de verplichtingen van de verwerkingsverantwoordelijke overeenkomstig hoofdstuk IV?

d. Wordt op grond van de criteria bewijs verlangd voor de evaluatie en actualisering van technische en organisatorische maatregelen overeenkomstig artikel 24, lid 1?

e. Moet er op grond van de criteria worden gecontroleerd of de organisatie heeft beoordeeld of er een functionaris voor gegevensbescherming moet worden aangewezen overeenkomstig artikel 37? Voldoet de functionaris voor gegevensbescherming, waar passend, aan de vereisten van de artikelen 37 tot en met 39?

f. Moet er op grond van de criteria worden gecontroleerd of registers van verwerkingsactiviteiten moeten worden gehouden overeenkomstig artikel 30, lid 5, en op passende wijze aan de vereisten van artikel 30 wordt voldaan?

8 RECHTEN VAN DE BETROKKENEN

a. Komen de criteria tegemoet aan het recht op informatie van betrokkenen en moeten op grond van de criteria maatregelen worden getroffen?

b. Moeten betrokkenen op grond van de criteria passende of zelfs ruimere toegang hebben tot en controle hebben over hun gegevens, inclusief gegevensoverdraagbaarheid?

c. Moeten er op grond van criteria maatregelen worden getroffen die het mogelijk maken in de verwerking in te grijpen om de rechten van betrokkenen te waarborgen en correcties, wissen of beperkingen mogelijk te maken?

…

9 RISICO'S VOOR DE RECHTEN EN VRIJHEDEN VAN NATUURLIJKE PERSONEN

a. Bieden de criteria de mogelijkheid om de risico's voor de rechten en vrijheden van natuurlijke personen te beoordelen en vereisen zij dat?

b. Bieden of vereisen de criteria een erkende risicobeoordelingsmethode? Staat deze, indien gepast, in verhouding?

c. Bieden de criteria de mogelijkheid om het effect van de beoogde verwerkingen op de rechten en vrijheden van natuurlijke personen te beoordelen en vereisen zij dit?

d. Is er op grond van de criteria voorafgaande raadpleging vereist ten aanzien van de resterende risico's die niet konden worden verminderd, op basis van de uitkomsten van de gegevensbeschermingseffectbeoordeling?

10 TECHNISCHE EN ORGANISATORISCHE MAATREGELEN DIE BESCHERMING WAARBORGEN

a. Moeten er op grond van criteria technische en organisatorische maatregelen worden getroffen die de vertrouwelijkheid van verwerkingen moeten waarborgen?

b. Moeten er op grond van criteria technische en organisatorische maatregelen worden getroffen die de integriteit van verwerkingen moeten waarborgen?

c. Moeten er op grond van criteria technische en organisatorische maatregelen worden getroffen die de beschikbaarheid van verwerkingen moeten waarborgen?

d. Moeten er op grond van criteria maatregelen worden getroffen die de transparantie van verwerkingen moeten waarborgen ten aanzien van:

e. verantwoordingsplicht?

f. rechten van de betrokkenen?

g. beoordeling van individuele verwerkingen, bijvoorbeeld transparantie van algoritmen?

h. Moeten er op grond van criteria technische en organisatorische maatregelen worden getroffen die de rechten van betrokkenen, bijvoorbeeld de mogelijkheid om informatie te verstrekken of ten aanzien van gegevensoverdraagbaarheid, moeten waarborgen?

i. Moeten er op grond van criteria technische en organisatorische maatregelen worden getroffen die het mogelijk maken in de verwerking in te grijpen om de rechten van betrokkenen te waarborgen en correcties, wissen of beperkingen mogelijk te maken?

j. Moeten er op grond van criteria maatregelen worden getroffen die het mogelijk maken in de verwerking in te grijpen om het systeem of het proces te herstellen of te controleren?

k. Moeten er op grond van criteria technische en organisatorische maatregelen worden getroffen die minimale gegevensverwerking, bijvoorbeeld ontkoppeling of scheiding van gegevens en betrokkenen, anonimisering of pseudonimisering of isolatie van gegevenssystemen, waarborgen?

l. Moeten er op grond van criteria technische maatregelen worden getroffen om standaard gegevensbescherming uit te voeren?

m. Moeten er op grond van criteria technische en organisatorische maatregelen worden getroffen voor de uitvoering van gegevensbescherming door ontwerp, bijvoorbeeld een beheerssysteem voor gegevensbescherming om gegevensbeschermingsvereisten aan te tonen, te controleren, te handhaven en hierover te informeren?

n. Moeten er op grond van criteria technische en organisatorische maatregelen worden getroffen voor de uitvoering van passende periodieke opleidingen en onderwijs voor personeel dat permanent of op regelmatige basis toegang heeft tot persoonsgegevens?

o. Moeten er op grond van criteria maatregelen voor evaluatie worden getroffen?

p. Moet er op grond van criteria zelfbeoordeling / intern onderzoek plaatsvinden?

q. Moeten er op grond van criteria maatregelen worden getroffen om te waarborgen dat verplichtingen ten aanzien van meldingen van inbreuk in verband met persoonsgegevens tijdig en binnen het toepassingsgebied plaatsvinden?

r. Moeten er op grond van criteria procedures voor incidentenbeheer worden ingesteld en gecontroleerd?

s. Moet er op grond van criteria toezicht worden gehouden op lopende privacy- en technologiekwesties en moet de regeling desgewenst worden geactualiseerd?

…

11 ANDERE BIJZONDERE GEGEVENSBESCHERMINGSVRIENDELIJKE FUNCTIES

a. Moeten er op grond van criteria technieken voor de verbetering van gegevensbescherming worden toegepast? Daaronder kunnen criteria vallen op grond waarvan de gegevensbescherming moet worden verbeterd door risico's ten aanzien van persoonsgegevens en/of gegevensbescherming weg te nemen of te verminderen.

- *Voorbeeld: Criteria op grond waarvan de ontkoppelbaarheid moet worden verbeterd door gebruik van op de gebruiker gericht identiteitsbeheer, zoals op kenmerken gebaseerde gegevens, in plaats van op de organisatie gericht identiteitsbeheer, kunnen als een techniek voor de verbetering van gegevensbescherming worden beschouwd.*

b. Moeten er op grond van de criteria verbeterde controles van betrokkenen worden uitgevoerd om zelfbeschikking en keuzevrijheid te bevorderen?

…

12 CRITERIA OM HET BESTAAN AAN TE TONEN VAN PASSENDE WAARBORGEN VOOR DE DOORGIFTE VAN PERSOONSGEGEVENS

Criteria komen aan de orde in komende richtsnoeren voor artikel 42, lid 2.

13 AANVULLENDE CRITERIA VOOR EEN EUROPEES GEGEVENSBESCHERMINGSZEGEL

a. Worden in de criteria alle lidstaten beoogd?

b. Kan er in de criteria rekening worden gehouden met gegevensbeschermingsrecht of -scenario's van de lidstaten?

c. Moet er op grond van de criteria een beoordeling van het individuele onderwerp van beoordeling plaatsvinden ten aanzien van sectorgebonden gegevensbeschermingsrecht van de lidstaten?

d. Moet op grond van de criteria de verwerkingsverantwoordelijke of verwerker informatie aan betrokkenen en belanghebbenden verstrekken in de talen van de lidstaten:

e. over de verwerking / het onderwerp van beoordeling?

f. documentatie over de verwerking / het onderwerp van beoordeling?

g. de resultaten van de beoordeling?

…

14 ALGEMENE BEOORDELING VAN CRITERIA

a. Bestrijken de criteria het gehele toepassingsgebied van het certificeringsmechanisme (d.w.z. uitgebreide criteria) om voldoende waarborgen te bieden voor een betrouwbare certificering?

- *Voorbeeld: Indien het toepassingsgebied van het certificeringsmechanisme zich richt op verwerkingen op het gebied van gezondheid, moet een hoog niveau van gegevensbescherming worden gewaarborgd door het vaststellen van criteria op grond waarvan bijvoorbeeld een grondige beoordeling plaatsvindt en beginselen van privacy door ontwerp en privacy door standaardinstellingen worden toegepast.*

b. Staan de criteria in verhouding tot de omvang van de verwerking die binnen het toepassingsgebied van het certificeringsmechanisme valt, de gevoeligheid van de informatie en het risico van de verwerking?

c. Is het waarschijnlijk dat de criteria een verbetering zullen opleveren voor de naleving van gegevensbescherming door verwerkingsverantwoordelijken en verwerkers?

d. Zullen betrokkenen hierbij baat hebben wat betreft hun informatierechten, inclusief de uitleg van gewenste uitkomsten aan betrokkenen?