Advies 21/2020 over het ontwerpbesluit van de bevoegde toezichthoudende autoriteit van Nederland betreffende de goedkeuring van de eisen inzake de accreditatie van een certificeringsorgaan overeenkomstig artikel 43, lid 3, van de AVG

Vastgesteld op 23 juli 2020

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Inhoudsopgave

Het Europees Comité voor gegevensbescherming

Gezien artikel 63, artikel 64, lid 1, onder c), en leden 3 tot en met 8, en artikel 43, lid 3, 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 met name bijlage XI en protocol 37, zoals gewijzigd bij Besluit nr. 154/2018 van het Gemengd Comité van de EER van 6 juli 2018[1],

Gezien de artikelen 10 en 22 van zijn reglement van orde van 25 mei 2018,

Overwegende hetgeen volgt:

(1) De voornaamste taak van het Comité is om te zorgen voor een consistente toepassing van Verordening (EU) 2016/679 (hierna: "de AVG") in de gehele Europese Economische Ruimte. In overeenstemming met artikel 64, lid 1, van de AVG brengt het Comité een advies uit wanneer een toezichthoudende autoriteit voornemens is de eisen vast te stellen voor de accreditatie van certificeringsorganen overeenkomstig artikel 43. Het doel van dit advies is derhalve te zorgen voor een geharmoniseerde aanpak met betrekking tot de eisen die een toezichthoudende autoriteit voor gegevensbescherming of de nationale accreditatie-instantie toepast voor de accreditatie van een certificeringsorgaan. Hoewel de AVG niet voorziet in één reeks verplichte eisen voor accreditatie, is zij er wel op gericht coherentie te bevorderen. Het Comité streeft ernaar deze doelstelling te met zijn adviezen te verwezenlijken door ten eerste toezichthoudende autoriteiten aan te moedigen hun eisen voor accreditatie op te stellen overeenkomstig de indeling in de bijlage bij de richtsnoeren van het EDPB inzake de accreditatie van certificeringsorganen en door ten tweede ze te analyseren met behulp van een door het EDPB verstrekt model aan de hand waarvan de eisen kunnen worden gebenchmarkt (op basis van ISO 17065 en de richtsnoeren van het EDPB inzake de accreditatie van certificeringsorganen).

(2) Volgens artikel 43 van de AVG worden de accreditatie-eisen vastgesteld door de bevoegde toezichthoudende autoriteiten. Ze passen hierbij echter het coherentiemechanisme toe om ervoor te zorgen dat er vertrouwen ontstaat in het certificeringsmechanisme, met name door een hoog niveau van eisen vast te stellen.

(3) Hoewel de accreditatie-eisen worden vastgesteld met inachtneming van het coherentiemechanisme, betekent dit niet dat de eisen identiek moeten zijn. De bevoegde toezichthoudende autoriteiten hebben een beoordelingsmarge met betrekking tot de nationale of regionale context en moeten rekening houden met hun lokale wetgeving. Het doel van het advies van het EDPB is niet de totstandbrenging van één enkele reeks eisen voor de EU, maar de voorkoming van aanzienlijke inconsistenties die bijvoorbeeld van invloed kunnen zijn op het vertrouwen in de onafhankelijkheid of deskundigheid van geaccrediteerde certificeringsorganen.

[1] Alle verwijzingen in dit advies naar de "Unie" moeten worden gelezen als verwijzingen naar de "EER".

(4) De "Richtsnoeren 4/2018 inzake de accreditatie van certificeringsorganen op grond van artikel 43 van de algemene verordening gegevensbescherming (2016/679)" (hierna: "de richtsnoeren") en de "Richtsnoeren van 1/2018 voor certificering en het vaststellen van certificeringscriteria overeenkomstig de artikelen 42 en 43 van de verordening" dienen als rode draad in het kader van het coherentiemechanisme.

(5) Indien een lidstaat bepaalt dat de certificeringsorganen door de toezichthoudende autoriteit moeten worden geaccrediteerd, dient de toezichthoudende autoriteit accreditatie-eisen vast te stellen die onder meer ook de in artikel 43, lid 2, van de AVG vermelde eisen omvatten. De regelingen van artikel 43 betreffende de eisen voor accreditatie, die van toepassing zijn wanneer de toezichthoudende autoriteit zelf de accreditatie ter hand neemt, zijn minder gedetailleerd dan de verplichtingen die gelden in het geval van accreditatie van certificeringsorganen door nationale accreditatie-instanties. Teneinde bij te dragen aan een geharmoniseerde benadering van accreditatie moet ISO/IEC 17065 leidend zijn voor de door de toezichthoudende autoriteit gehanteerde accreditatie-eisen en moeten deze worden aangevuld met de aanvullende eisen die een toezichthoudende autoriteit vaststelt op grond van artikel 43, lid 1, onder b). Het EDPB merkt op dat artikel 43, lid 2, onder a) tot en met e), de eisen van ISO 17065 weerspiegelen en specificeren, hetgeen de coherentie ten goede komt.[2]

(6) Het advies van het EDPB zal overeenkomstig artikel 64, lid 1, onder c, en leden 3 en 8, van de AVG in samenhang met artikel 10, lid 2, van het reglement van orde van het EDPB worden vastgesteld binnen acht weken na de eerste werkdag nadat de voorzitter en de bevoegde toezichthoudende autoriteit hebben besloten dat het dossier volledig is. De voorzitter kan besluiten deze termijn met zes weken te verlengen, rekening houdend met de complexiteit van de aangelegenheid.

HEEFT HET VOLGENDE ADVIES VASTGESTELD:

1 SAMENVATTING VAN DE FEITEN

1. De toezichthoudende autoriteit van Nederland (hierna: "Nederlandse toezichthouder") heeft haar ontwerp van de accreditatie-eisen overeenkomstig artikel 43, lid 1, onder b), ingediend bij het EDPB. Het dossier is op 28 mei 2020 als volledig aangemerkt. De nationale accreditatie-instantie van Nederland wordt belast met de accreditatie van certificeringsorganen met het oog op certificatie overeenkomstig de in de AVG vastgestelde certificeringscriteria. Dit houdt in dat de nationale accreditatie-instantie bij de accreditatie van certificeringsorganen ISO 17065 zal toepassen, evenals de door de Nederlandse toezichthouder geformuleerde aanvullende eisen, nadat deze voor door de Nederlandse toezichthouder zijn vastgesteld na een advies van het Comité over de ontwerpeisen.

[2] Richtsnoeren 4/2018 inzake de accreditatie van certificeringsorganen op grond van artikel 43 van de algemene verordening gegevensbescherming (2016/679), punt 39. Beschikbaar op: https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en

2 BEOORDELING

2.1 Algemene redenering van het EDPB met betrekking tot het ingediende ontwerpbesluit

2. Het doel van dit advies is de beoordeling van de accreditatie-eisen die zijn ontwikkeld door een toezichthoudende autoriteit, hetzij in verband met ISO 17065, hetzij als volledige reeks eisen, om een nationale accreditatie-instantie of een toezichthoudende autoriteit, overeenkomstig artikel 43, lid 1, van de AVG, in staat te stellen een certificeringsorgaan te accrediteren dat verantwoordelijk is voor de verstrekking en verlenging van certificeringen in overeenstemming met artikel 42 van de AVG. Dit wordt gedaan onverminderd de taken en bevoegdheden van de bevoegde toezichthoudende autoriteit. In dit specifieke geval merkt het Comité op dat de Nederlandse toezichthouder heeft besloten zijn nationale accreditatie-instantie te belasten met de afgifte van accreditaties en dat hij in overeenstemming met de richtsnoeren aanvullende eisen heeft opgesteld, die door de nationale accreditatie-instantie moeten worden gehanteerd bij de afgifte van accreditaties.

3. Deze beoordeling van de aanvullende accreditatie-eisen van de Nederlandse toezichthouder is gericht op het onderzoek van afwijkingen (toevoegingen of schrappingen) van de richtsnoeren, en met name van bijlage 1 daarbij. Daarnaast is het advies van het EDPB ook gericht op alle aspecten die van invloed kunnen zijn op een coherente benadering van de accreditatie van certificeringsorganen.

4. Er moet worden opgemerkt dat het doel van de richtlijnen betreffende de accreditatie van certificeringsorganen erin bestaat de toezichthoudende autoriteiten te ondersteunen bij het vaststellen van hun accreditatie-eisen. De bijlage bij de richtsnoeren behelst op zich geen accreditatie-eisen. Derhalve moeten de accreditatie-eisen voor certificeringsorganen worden gedefinieerd door de toezichthoudende autoriteit op een manier die de praktische en coherente toepassing ervan mogelijk maakt, zoals vereist in de context van de toezichthoudende autoriteit.

5. Het Comité erkent het feit dat er, gelet op hun deskundigheid, manoeuvreerruimte moet worden toegekend aan de nationale accreditatie-instanties bij het definiëren van bepaalde specifieke bepalingen binnen de toepasselijke accreditatie-eisen. Het Comité acht het echter noodzakelijk om te benadrukken dat, wanneer er aanvullende eisen zijn opgesteld, deze zo moeten worden gedefinieerd dat ze op praktische en consistente wijze kunnen worden toegepast en indien nodig herzien.

6. Het Comité merkt op dat op ISO-normen, met name ISO 17065, intellectuele-eigendomsrechten van toepassing zijn en verwijst derhalve niet naar de tekst van het gerelateerde document in dit advies. Daarom heeft het Comité besloten om, indien relevant, te verwijzen naar specifieke punten van de ISO-norm, zonder echter de tekst te reproduceren.

7. Tot slot heeft het Comité zijn beoordeling uitgevoerd in overeenstemming met de structuur die is vastgelegd in bijlage 1 bij de richtsnoeren (hierna: “de bijlage”). Indien in dit advies een specifiek deel van het ontwerp van de accreditatie-eisen van de Nederlandse toezichthouder niet aan bod komt, houdt dit in dat het Comité geen opmerkingen heeft en de Nederlandse toezichthouder niet verzoekt om nadere actie te ondernemen.

8. Dit advies gaat niet in op door de Nederlandse toezichthouder ingediende onderdelen die buiten het toepassingsgebied van artikel 43, lid 2, van de AVG vallen, zoals verwijzingen naar de nationale wetgeving. Het Comité merkt evenwel op dat de nationale wetgeving waar nodig in overeenstemming met de AVG moet zijn.

2.2 Belangrijkste focuspunten voor de beoordeling (art. 43, lid 2, van de AVG en bijlage 1 bij de EDPB-richtsnoeren) opdat de accreditatie-eisen waarborgen dat de volgende elementen op coherente wijze worden beoordeeld:

a. alle belangrijke voorwaarden, zoals vermeld in de bijlage bij de richtsnoeren, komen aan bod en eventuele afwijkingen van de bijlage worden gemotiveerd;

b. de onafhankelijkheid van het certificeringsorgaan;

c. belangenverstrengeling bij het certificeringsorgaan;

d. de deskundigheid van het certificeringsorgaan;

e. passende waarborgen om ervoor te zorgen dat de in de AVG vastgestelde certificeringscriteria op passende wijze worden toegepast door het certificeringsorgaan;

f. procedures voor de verlening, periodieke herziening en intrekking van AVG-certificering; en

g. transparante afhandeling van klachten over inbreuken op de certificering.

9. Overwegende dat:

a. artikel 43, lid 2, van de AVG een lijst bevat van accreditatievoorwaarden waaraan een certificeringsorgaan moet voldoen om te worden geaccrediteerd,

b. in artikel 43, lid 3, van de AVG is bepaald dat de eisen voor de accreditatie van certificeringsorganen worden vastgesteld door de bevoegde toezichthoudende autoriteit,

c. in artikel 57, lid 1, onder p) en q), van de AVG is bepaald dat een bevoegde toezichthoudende autoriteit de accreditatie-eisen voor certificeringsorganen moet opstellen en bekendmaken en kan besluiten de accreditatie van certificeringsorganen zelf uit te voeren,

d. in artikel 64, lid 1, onder c), van de AVG is bepaald dat het Comité een advies uitbrengt wanneer een toezichthoudende autoriteit voornemens is de eisen vast te stellen voor de accreditatie van certificeringsorganen overeenkomstig artikel 43, lid 3,

e. indien de accreditatie wordt uitgevoerd door de nationale accreditatie-instantie overeenkomstig ISO/IEC 17065/2012, tevens de door de bevoegde toezichthoudende autoriteit vastgestelde aanvullende eisen moeten worden toegepast,

f. bijlage 1 bij de richtsnoeren over de accreditatie van certificeringsorganen voorziet in voorgestelde eisen die een toezichthoudende autoriteit voor gegevensbescherming moet opstellen en die van toepassing zijn tijdens de accreditatie van een certificeringsorgaan door de nationale accreditatie-instantie,

is het Comité de volgende mening toegedaan:

2.2.1 ALGEMENE OPMERKINGEN

10. Het Comité constateert dat de ontwerpeisen van de Nederlandse toezichthouder een artikel bevatten over termen en definities. Sommige termen worden echter niet consequent in het hele document gebruikt (bv. “object of evaluation” (“onderwerp van beoordeling”) én “ToE” , “accreditation body” (“accreditatie-instantie”) én “RvA”, de term “CB” wordt niet in de tekst gebruikt en in de tekst is soms sprake van “the competent supervisory authority” (“de bevoegde toezichthoudende autoriteit”) in plaats van de “NL SA” (“Nederlandse toezichthouder”) ...). Daarnaast is het Comité van mening dat bij verwijzingen naar ISO 17065 de desbetreffende punten moeten worden vermeld. Hoewel dit hier en daar wel gebeurt (bv. in de artikelen 7.3, 7.5, 7.6, 7.7 en 7.9 van de ontwerpeisen van de Nederlandse toezichthouder), is dit niet overal in het document consequent het geval (onder meer in de artikelen 4.2, 4.3, 4.6, 6.2, 7.1, 7.2, 7.4 en 7.8 van de ontwerpeisen van de Nederlandse toezichthouder worden de relevante punten van ISO 17065 niet vermeld). Het Comité spoort de Nederlandse toezichthouder aan zorg te dragen voor consequent gebruik van termen en duidelijke verwijzingen naar ISO 17065.

11. Het Comité merkt op dat sommige artikelen van de bijlage ontbreken (bv. artikel 9.3.2 van de bijlage “Documentation of evaluation activities” (“Documentatie van evaluatieactiviteiten”)). Het Comité gaat ervan uit dat in die gevallen geen aanvullende eisen werden geformuleerd. Omwille van de duidelijkheid moedigt het Comité de Nederlandse toezichthouder echter aan de ontbrekende artikelen toe te voegen of een verklaring aan het begin van de ontwerpeisen op te nemen, waarin wordt verduidelijkt dat in gevallen waarin bepaalde artikelen ontbreken geen aanvullende eisen zijn geformuleerd.

2.2.2 ALGEMENE ACCREDITATIE-EISEN

12. Het Comité merkt op dat in de laatste alinea van artikel 4.1.1 van het ontwerp van de accreditatie-eisen van de Nederlandse toezichthouder (“Legal responsibility” – “Wettelijke aansprakelijkheid”) wordt verwezen naar onderzoeken of regelgevende maatregelen *“met betrekking tot het onderwerp van beoordeling die kunnen inhouden dat zij niet aan deze eis voldoen en derhalve in de weg kunnen staan aan hun accreditatie” (“in relation to the subject matter of the ToE which may mean they do not meet this requirement and therefore might prevent their accreditation”).* Het Comité is van oordeel dat de verwijzing naar het onderwerp van beoordeling in dit geval niet geheel correct is, aangezien de eis betrekking heeft op de accreditatie van de certificeringsorganen en niet op hun certificeringsactiviteiten. Daarom moedigt het Comité de Nederlandse toezichthouder aan deze verwijzing in het laatste deel van de eis te schrappen.

13. Met betrekking tot artikel 4.1.2 van het ontwerp van de accreditatie-eisen van de Nederlandse toezichthouder (“Certification agreement” – “Certificeringsovereenkomst”), merkt het Comité op dat punt 6 niet alle elementen van punt 8 van de bijlage bevat. Met name “de nodige voorzorgsmaatregelen voor het onderzoek van klachten” (“the necessary precautions for the investigation of complaints”) ontbreken. Het Comité beveelt de Nederlandse toezichthouder aan de ontbrekende informatie in de bijlage op te nemen.

14. Daarnaast is het Comité van mening dat punt 7 van artikel 4.1.2 met betrekking tot de verplichting van de aanvrager om het certificeringsorgaan in kennis te stellen van relevante inbreuken op de AVG of de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) moet worden verduidelijkt. Het Comité is van mening dat deze verplichting niet mag leiden tot zelfincriminatie en dat de verplichting derhalve betrekking moet hebben op door de Nederlandse toezichthouder en/of rechterlijke instanties vastgestelde inbreuken. Het Comité beveelt de Nederlandse toezichthouder

derhalve aan een dergelijke verduidelijking aan te brengen. Om verwarring te voorkomen, moedigt het Comité de Nederlandse toezichthouder bovendien aan te verduidelijken dat "relevante inbreuken" ("relevant infringements") betrekking hebben op inbreuken op de AVG of de UAVG die van invloed kunnen zijn op certificering.

15. Met betrekking tot punt 9 van artikel 4.1.2, merkt het Comité op dat er een verwijzing naar de gevolgen voor de betrokkenen is opgenomen. De Nederlandse toezichthouder heeft echter geen verwijzing opgenomen naar het vereiste [indien van toepassing] dat "ook rekening moet worden gehouden met alle gevolgen voor [de] klanten", zoals vermeld in de bijlage. Het Comité beveelt de Nederlandse toezichthouder derhalve aan de term door "klant" ("customer") te vervangen om de formulering in overeenstemming te brengen met de bijlage.

16. Met betrekking tot punt 4.3 ("Aansprakelijkheid en financiering") van het ontwerp van de accreditatie-eisen van de Nederlandse toezichthouder, merkt het Comité op dat het certificeringsorgaan, in overeenstemming met de bijlage, op regelmatige basis moet aantonen dat het passende maatregelen heeft ingevoerd om zijn aansprakelijkheid te dekken. In het ontwerp van de accreditatie-eisen van de Nederlandse toezichthouder is de zinsnede "op regelmatige basis" niet opgenomen en daarom beveelt het Comité de Nederlandse toezichthouder aan een dergelijke formulering op te nemen, in overeenstemming met de bijlage.

17. Het Comité merkt op dat artikel 4.3 van het ontwerp van de accreditatie-eisen van de Nederlandse toezichthouder de verplichting bevat dat het certificeringsorgaan moet aantonen over voldoende financiële middelen te beschikken opdat gewaarborgd is dat de geldboeten die kunnen worden opgelegd op grond van artikel 83, lid 4, onder b), van de AVG, worden betaald. Het Comité is van mening dat deze specifieke verwijzing naar de geldboeten in het kader van de AVG in de praktijk tot een aantal problemen kan leiden, met name wat betreft de beoordeling van de naleving van de vereisten. Het Comité moedigt de Nederlandse toezichthouder dan ook aan de specifieke verwijzing naar geldboeten in het kader van de AVG te heroverwegen, rekening houdend met de mogelijke praktische moeilijkheden die een dergelijke verwijzing met zich mee kan brengen.

18. Het Comité merkt op dat in artikel 4.6 van het ontwerp van de accreditatie-eisen van de Nederlandse toezichthouder ("Openbaar beschikbare informatie") de verplichting is opgenomen om aan te tonen dat de goedgekeurde criteria zijn gepubliceerd en dat de "certificeringsprocedures uitvoerig moeten worden toegelicht" ("high-level explanations about the certification procedures"). Het Comité merkt op dat een "uitvoerige" toelichting ontoereikend kan blijken om de in de bijlage vereiste informatie te verstrekken. Daarom moedigt het Comité de Nederlandse toezichthouder aan toe te voegen dat "ter zake dienende" toelichtingen zullen worden verstrekt.

2.2.3 BENODIGDE MIDDELEN

19. Met betrekking tot het personeel van de certificeringsorganen (artikel 6.1 van het ontwerp van de accreditatie-eisen van de Nederlandse toezichthouder) merkt het Comité op dat de eisen in overeenstemming zijn met de bijlage. In dit verband is het Comité van mening dat, met betrekking tot de deskundigheid van het certificeringsorgaan, de nadruk moet worden gelegd op de verschillende soorten materiële deskundigheid en ervaring. Het Comité is met name van mening dat de deskundigheidseisen voor evaluatoren en besluitvormers moeten worden afgestemd op de verschillende taken die zij uitvoeren. Het Comité is van mening dat evaluatoren meer specialistische kennis en professionele ervaring moeten hebben met technische procedures (zoals audits en

certificeringen), terwijl besluitvormers moeten beschikken over een meer algemene en uitgebreidere kennis en professionele ervaring op het gebied van gegevensbescherming. In dit licht moedigt het Comité de Nederlandse toezichthouder aan dit deel te herschrijven en daarbij rekening te houden met de verschillende eisen op het vlak van inhoudelijke kennis en/of ervaring voor evaluatoren en besluitvormers.

20. Daarnaast merkt het Comité op dat de bijlage met betrekking tot personeel met juridische expertise een specifieke opleiding of significante beroepservaring vereist. Deze laatste verwijzing ontbreekt in het ontwerp van de accreditatie-eisen van de Nederlandse toezichthouder. Het Comité beveelt de Nederlandse toezichthouder aan een dergelijke verwijzing toe te voegen.

21. Met betrekking tot de onderwijsvereisten voor personeel met technische expertise, wordt in de bijlage bovendien verwezen naar "een kwalificatie op een relevant gebied van technische deskundigheid op ten minste EQF-niveau 6 of een erkende beschermde titel (bv. Dpl. Ing.) voor het betrokken gereglementeerde beroep". Het Comité merkt op dat het ontwerp van de accreditatie-eisen van de Nederlandse toezichthouder geen verwijzing bevat naar een erkende beschermde titel voor het betrokken gereglementeerde beroep en beveelt de Nederlandse toezichthouder aan een dergelijke verwijzing op te nemen.

2.2.4 PROCESVEREISTEN

22. Met betrekking tot artikel 7.2 ("Aanvraag") van het ontwerp van de accreditatie-eisen van de Nederlandse toezichthouder, merkt het Comité op dat in punt 4 de verplichting is opgenomen om "*alle lopende of recente onderzoeken of regelgevende maatregelen die op de aanvrager van toepassing zijn, openbaar te maken*" ("*disclose any current or recent AP investigation or regulatory action to which the applicant is subject"*). Het Comité is van mening dat de verplichting moet worden afgestemd op onderzoeken of regelgevende maatregelen die verband houden met het toepassingsgebied van de certificering en het doel van de evaluatie. Het Comité moedigt de Nederlandse toezichthouder derhalve aan te verduidelijken dat het onderzoek of de regelgevende maatregel verband moet houden met het toepassingsgebied van de certificering en het doel van de evaluatie.

23. Met betrekking tot punt 3 van artikel 7.4 ("Evaluatie"), is het Comité van mening dat met de verwijzing naar de eisen "zoals uiteengezet in de criteria" ("as set out in the criteria") lijkt te worden verondersteld dat de criteria volledig zijn. Het Comité erkent dat de Nederlandse toezichthouder de formulering van de bijlage heeft gebruikt, maar moedigt de Nederlandse toezichthouder aan te verwijzen naar "de vastgestelde criteria" om verwarring te voorkomen.

24. Het Comité merkt op dat in de tweede alinea van artikel 7.6 van het ontwerp van de accreditatie-eisen van de Nederlandse toezichthouder ("certificeringsbesluit") de verplichting is opgenomen om het ontwerp van goedkeuring aan de Nederlandse toezichthouder voor te leggen alvorens certificering af te geven of te verlengen. Op basis van de uitleg van de Nederlandse toezichthouder begrijpt het Comité dat het de bedoeling van deze eis is de transparantie te vergroten en dat deze geen toezicht op het ontwerp van goedkeuring inhoudt. Het Comité moedigt de Nederlandse toezichthouder aan een verduidelijking in die zin op te nemen.

25. Met betrekking tot artikel 7.10 van het ontwerp van de accreditatie-eisen van de Nederlandse toezichthouder ("Wijzigingen die van invloed zijn op de certificering"), merkt het Comité op dat in het

eerste punt “elke inbreuk in verband met persoonsgegevens of inbreuk op de AVG” (“any personal data breach or infringement of the GDPR”) is opgenomen. Het Comité is van mening dat, om zelfincriminatie te voorkomen, moet worden verwezen naar door de Nederlandse toezichthouder of de bevoegde rechterlijke instantie vastgestelde inbreuken. Bovendien lijkt de formulering “elke inbreuk in verband met persoonsgegevens” (“any data breach”) vrij ruim. Het Comité is van mening dat een dergelijke formulering verder moet worden uitgewerkt zodat wordt verduidelijkt of ook kleine inbreuken in verband met persoonsgegevens moeten worden gemeld. Daarom moedigt het Comité de Nederlandse toezichthouder aan de formulering te wijzigen door te verwijzen naar “vastgestelde” (“established”) inbreuken en de betekenis van “elke inbreuk in verband met persoonsgegevens” (“any data breach”) te verduidelijken.

26. Het Comité merkt op dat de eerste zin van artikel 7.11 niet als een dwingende eis is geformuleerd. Het Comité moedigt de Nederlandse toezichthouder aan het woord “dient” (“should”) te vervangen door “moet” (“shall”) om duidelijk te maken dat dit een verplichting is. Daarnaast merkt het Comité op dat de verplichting om informatie te verstrekken over de genomen maatregelen ook geldt voor de nationale accreditatie-instantie, zoals vermeld in de bijlage. Het Comité beveelt de Nederlandse toezichthouder aan een dergelijke verwijzing naar de nationale accreditatie-instantie toe te voegen.

27. Ten slotte wordt in artikel 7.13 van het ontwerp van de accreditatie-eisen van de Nederlandse toezichthouder (“Klachten en beroepen”) bepaald dat de klager binnen een maand na ontvangst van de klacht in kennis moet worden gesteld van de voortgang en het resultaat van de klacht. Hoewel transparantie ten aanzien van klagers van groot belang is, is het Comité van mening dat een strikte verplichting om de klager het resultaat van de klacht binnen een maand mee te delen, onrealistische verwachtingen kan doen ontstaan en een grote uitdaging kan vormen voor het certificeringsorgaan. Daarom moedigt het Comité de Nederlandse toezichthouder aan de eisen te herformuleren door te bepalen dat het certificeringsorgaan de klagers binnen een maand na ontvangst van de klacht in kennis moet stellen van de voortgang of het resultaat.

2.2.5 EISEN MET BETREKKING TOT HET MANAGEMENTSYSTEEM

28. Met betrekking tot artikel 8 van het ontwerp van de accreditatie-eisen van de Nederlandse toezichthouder (“Eisen met betrekking tot het managementsysteem”), merkt het Comité op dat de verplichting voor het certificeringsorgaan om de Nederlandse toezichthouder in kennis te stellen van de beheerbeginselen en de gedocumenteerde tenuitvoerlegging ervan tijdens de accreditatieprocedure niet is voorzien. Het Comité beveelt de Nederlandse toezichthouder aan de ontwerpeisen te wijzigen door een dergelijke verplichting op te nemen, zoals vermeld in de bijlage.

2.2.6 VERDERE AANVULLENDE EISEN

29. In artikel 9.3.2 van het ontwerp van de accreditatie-eisen van de Nederlandse toezichthouder (“Beheer van de behandeling van klachten”) is de verplichting niet opgenomen om relevante klachten en bezwaren met de Nederlandse toezichthouder te delen, zoals vermeld in de bijlage. Het Comité beveelt de Nederlandse toezichthouder aan om een dergelijke verplichting op te nemen.

3 CONCLUSIES/AANBEVELINGEN

30. Het ontwerp van de accreditatie-eisen van de Nederlandse toezichthoudende autoriteit kan leiden tot een incoherente toepassing van de accreditatie van certificeringsorganen. De volgende wijzigingen moeten worden aangebracht:

31. Ten aanzien van de “algemene accreditatie-eisen” beveelt het Comité aan dat de Nederlandse toezichthouder:

    1) de ontbrekende informatie uit de verwijzingen in de bijlage toevoegt in punt 6 van artikel 4.1.2;

    2) in punt 7 van artikel 4.1.2 verduidelijkt dat de verplichting voor de aanvrager om het certificeringsorgaan in kennis te stellen van relevante inbreuken op de AVG of de Uitvoeringswet Algemene verordening gegevensbescherming betrekking moet hebben op door de Nederlandse toezichthouder en/of rechterlijke instanties vastgestelde inbreuken;

    3) de term in punt 9 van artikel 4.1.2 vervangt door “klant” (“customer”), om de formulering in overeenstemming te brengen met de bijlage;

    4) in artikel 4.3 een verwijzing opneemt naar het begrip “op regelmatige basis”, in overeenstemming met de bijlage.

32. Ten aanzien van de “benodigde middelen” beveelt het Comité aan dat de Nederlandse toezichthouder:

    1) in artikel 6.1 een verwijzing toevoegt naar aanzienlijke beroepservaring met betrekking tot personeel met juridische expertise;

    2) in de opleidingseisen voor personeel met technische deskundigheid, een verwijzing toevoegt naar een erkende beschermde titel voor het betrokken gereglementeerde beroep.

33. Ten aanzien van de “procesvereisten” beveelt het Comité aan dat de Nederlandse toezichthouder:

    1) in artikel 7.11 de verplichting toevoegt om de nationale accreditatie-instantie overeenkomstig de bijlage in kennis te stellen van de genomen maatregelen.

34. Ten aanzien van de “eisen met betrekking tot het managementsysteem” beveelt het Comité aan dat de Nederlandse toezichthouder:

    1) in artikel 8 de verplichting opneemt om de Nederlandse toezichthouder in kennis te stellen van de beheerbeginselen en de gedocumenteerde tenuitvoerlegging ervan tijdens de accreditatieprocedure.

35. Ten aanzien van de “verdere aanvullende eisen” beveelt het Comité aan dat de Nederlandse toezichthouder:

    1) in artikel 9.3.2 de verplichting opneemt om relevante klachten en bezwaren met de Nederlandse toezichthouder te delen, zoals vermeld in de bijlage.

4 SLOTOPMERKINGEN

36. Dit advies is gericht tot de Nederlandse toezichthoudende autoriteit en wordt bekendgemaakt op grond van artikel 64, lid 5, onder b), van de AVG.

37. Overeenkomstig artikel 64, leden 7 en 8, van de AVG deelt de Nederlandse toezichthoudende autoriteit de voorzitter binnen twee weken na ontvangst van het advies langs elektronische weg mee of zij haar ontwerplijst zal wijzigen dan wel handhaven. Binnen dezelfde termijn verstrekt zij de gewijzigde ontwerplijst of, indien zij niet voornemens is het advies van het Comité op te volgen, geeft zij de redenen op waarom zij voornemens is het advies geheel of gedeeltelijk niet op te volgen.

38. De Nederlandse toezichthoudende autoriteit deelt het uiteindelijke besluit aan het Comité mee zodat het overeenkomstig artikel 70, lid 1, onder y), van de AVG kan worden opgenomen in het register van in het kader van het coherentiemechanisme vastgestelde besluiten.

Voor het Europees Comité voor gegevensbescherming

De voorzitter

(Andrea Jelinek)

Vastgesteld