Advies van de EDPB (artikel 64)

Advies 15/2020 over het ontwerpbesluit van de bevoegde toezichthoudende autoriteiten van Duitsland betreffende de goedkeuring van de accreditatie-eisen van een certificeringsorgaan overeenkomstig artikel 43, lid 3, AVG

Vastgesteld op 25 mei 2020

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Vastgesteld

Inhoudsopgave

Het Europees Comité voor gegevensbescherming

Gezien artikel 63, artikel 64, lid 1, onder c), 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"),

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 rol van het Comité is te zorgen voor een consequente toepassing van de AVG binnen de gehele Europese Economische Ruimte. In overeenstemming met artikel 64, lid 1, AVG brengt het Comité een advies uit wanneer een toezichthoudende autoriteit voornemens is de eisen vast te stellen voor de accreditatie van certificeringsorganen krachtens 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, streeft zij er wel naar coherentie te bevorderen. Het Comité streeft ernaar deze doelstelling met zijn adviezen te verwezenlijken door ten eerste toezichthoudende autoriteiten aan te moedigen hun eisen voor accreditatie op te stellen overeenkomstig de indeling in bijlage 1 bij de richtsnoeren 4/2018 betreffende de accreditatie van certificeringsorganen van het EDPB en ten tweede door 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 betreffende de accreditatie van certificeringsorganen).

(2) Overeenkomstig artikel 43, 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.

(4) De "Richtsnoeren 4/2018 betreffende de accreditatie van certificeringsorganen op grond van artikel 43 van de algemene verordening gegevensbescherming (2016/679)" (hierna: "de

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

richtsnoeren") en de "Richtsnoeren 1/2018 betreffende certificering en het identificeren van certificeringscriteria overeenkomstig artikel 42 en 43 van Verordening 2016/679" 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, moet de toezichthoudende autoriteit accreditatie-eisen vaststellen, die onder meer ook de in artikel 43, lid 2, 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 de leden 3 en 8, 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 Duitse toezichthoudende autoriteiten van de Federatie en de Länder (hierna: "Duitse toezichthoudende autoriteiten") hebben hun ontwerp van de accreditatie-eisen krachtens artikel 43, lid 1, onder b), ingediend bij het EDPB. Het dossier is op 13 februari 2020 als volledig aangemerkt. De nationale accreditatie-instantie van Duitsland, Dakks, voert de accreditatie van de te certificeren certificeringsorganen uit met behulp van de certificeringscriteria in de AVG. Dit houdt in dat de nationale accreditatie-instantie voor het accrediteren van certificeringsinstanties gebruik zal maken van ISO 17065 en de aanvullende eisen van de Duitse toezichthoudende autoriteiten, zodra deze na advies van het Comité over de ontwerpeisen door de Duitse toezichthoudende autoriteiten zijn vastgesteld.

2. In overeenstemming met artikel 10, lid 2, van het reglement van orde van het Comité heeft de voorzitter vanwege de complexiteit van de onderhavige zaak besloten de aanvankelijke periode van acht weken voor vaststelling van het advies te verlengen met nog eens zes weken.

[2] Richtsnoeren 4/2018 betreffende de accreditatie van certificeringsinstanties op grond van artikel 43 van de algemene verordening gegevensbescherming, punt 39. Beschikbaar op: https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_nl

2 BEOORDELING

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

3. 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, AVG, in staat te stellen een certificeringsorgaan te accrediteren dat verantwoordelijk is voor de verstrekking en verlenging van certificeringen in overeenstemming met artikel 42, AVG. Dit wordt gedaan onverminderd de taken en bevoegdheden van de bevoegde toezichthoudende autoriteit. In dit specifieke geval merkt het Comité op dat de Duitse toezichthoudende autoriteiten hebben besloten de uitgifte van accreditaties onder te brengen bij de nationale accreditatie-instantie, DAkks, en de bevoegde toezichthoudende autoriteit gezamenlijk. De Duitse toezichthoudende autoriteiten hebben aanvullende eisen opgesteld in overeenstemming met de richtsnoeren die moeten worden gebruikt bij de uitgifte van accreditaties.

4. Deze beoordeling van de aanvullende accreditatie-eisen van de Duitse toezichthoudende autoriteiten is gericht op het onderzoek van variaties (toevoegingen of schrappingen) op de richtsnoeren en met name 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.

5. 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 autoriteiten op een manier die de praktische en coherente toepassing ervan mogelijk maakt, zoals vereist in de context van de toezichthoudende autoriteiten.

6. Het Comité erkent het feit dat er, gelet op hun deskundigheid, manoeuvreerruimte moet worden toegekend aan de nationale accreditatie-instanties en, indien van toepassing, de bevoegde toezichthoudende autoriteiten 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.

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

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

9. Dit advies gaat niet in op door de Duitse toezichthoudende autoriteiten ingediende zaken die buiten het toepassingsgebied van artikel 43, lid 2, AVG liggen, 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, AVG en bijlage 1 bij de EDPB-richtsnoeren) opdat de accreditatie-eisen waarborgen dat de volgende elementen op coherente wijze worden beoordeeld:

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

2) de onafhankelijkheid van het certificeringsorgaan;

3) belangenverstrengeling bij het certificeringsorgaan;

4) de deskundigheid van het certificeringsorgaan;

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

6) procedures voor de verlening, periodieke herziening en intrekking van AVG-certificering; en

7) transparante afhandeling van klachten over inbreuken op de certificering.

10. Overwegende dat:

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

b. in artikel 43, lid 3, 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), 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), 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 krachtens 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 VOORBEPALING

11. Het Comité erkent het feit dat de samenwerkingsvoorwaarden die de relatie tussen een nationale accreditatie-instantie en zijn toezichthoudende autoriteiten voor gegevensbescherming beheersen, niet per se een eis zijn voor de accreditatie van certificeringsorganen. Ten behoeve van de volledigheid en transparantie is het Comité echter van mening dat dergelijke samenwerkingsvoorwaarden, indien aanwezig, bekend moeten worden gemaakt in een door de toezichthoudende autoriteit geschikt geacht formaat.

2.2.2 TERMEN EN DEFINITIES

12. Het Comité merkt op dat in hoofdstuk 3 ("definities") van het ontwerp van de accreditatie-eisen van de Duitse toezichthoudende autoriteiten wordt gedefinieerd welke soorten certificeringsregelingen zijn toegestaan, waarbij wordt gespecificeerd dat ze moeten voldoen aan de eisen van DIN EN ISO/IEC 17065. In dit verband moet erop worden gewezen dat in de delen 5.1 en 5.2 van de EDPB-richtsnoeren reeds uitgebreid is opgenomen wat in het kader van de AVG kan worden gecertificeerd. Het Comité erkent derhalve dat de Duitse toezichthoudende autoriteiten niet voornemens zijn te beperken wat is vermeld in de richtlijnen en dat de stellingen in hoofdstuk 3 van het ontwerp van de accreditatie-eisen van de Duitse toezichthoudende autoriteiten moet worden beschouwd als toepasselijk in het kader van deze accreditatie-eisen.

2.2.3 ALGEMENE OPMERKINGEN

13. Het Comité merkt op dat in het deel "Algemene opmerkingen" in het ontwerp van de accreditatie-eisen van de Duitse toezichthoudende autoriteiten wordt verwezen naar de "toestemming" voor de certificeringscriteria door het EDPB "in overeenstemming met artikel 63 en artikel 64, lid 1, onder c), AVG". Het Comité merkt op dat de AVG het EDPB niet de bevoegdheid verleend om "toestemming te verlenen" voor certificeringscriteria. Overeenkomstig de hiervoor vermelde artikelen kan het EDPB de certificeringscriteria echter wel goedkeuren. Het Comité beveelt de Duitse toezichthoudende autoriteiten derhalve aan om de verwijzing naar "toestemming door het EDPB" te schrappen en er zo voor te zorgen dat het ontwerp overeenstemt met de formulering in de AVG.

2.2.4 ALGEMENE EISEN VOOR ACCREDITATIE (hoofdstuk 4 van het ontwerp van de accreditatie-eisen)

14. Met betrekking tot de eis inzake wettelijke verantwoordelijkheid (deel 4.1 van het ontwerp van de accreditatie-eisen van de Duitse toezichthoudende autoriteiten) merkt het Comité op dat de Duitse toezichthoudende autoriteiten in het ondersteunende document toelichten dat er een verwachting bestaat dat het certificeringsorgaan beschikt over actuele procedures en dat er daarom geen behoefte bestaat aan nadere eisen in dat opzicht. Het Comité is echter van mening dat een verwachting de certificeringsorganen niet bindt aan het hebben van dergelijke procedures. Zoals is vastgesteld in deel 4.1.1 van de bijlage bij de richtsnoeren moet een certificeringsorgaan beschikken over geactualiseerde procedures die aantonen dat het handelt in overeenstemming met de in de accreditatievoorwaarden opgenomen wettelijke aansprakelijkheid. Bovendien moet het certificeringsorgaan als onderdeel van het certificeringsproces in staat zijn om bewijs over te leggen van met de AVG strokende procedures en maatregelen die specifiek zijn bedoeld voor de controle en

verwerking van de persoonsgegevens van de organisatie die cliënt is. Daarom raadt het Comité de Duitse toezichthoudende autoriteiten aan om het ontwerp van de eisen aan te passen om ze in overeenstemming te brengen met de richtsnoeren.

15. Met betrekking tot deel 4.1.2.2 van het ontwerp van de accreditatie-eisen van de Duitse toezichthoudende autoriteiten ("certificeringsovereenkomst") merkt het Comité op dat het ontwerp van de accreditatie-eisen van de Duitse toezichthoudende autoriteiten geen verplichting bevat om volledige transparantie te bieden aan de bevoegde toezichthoudende autoriteit met betrekking tot de certificeringsprocedure, ook wat betreft contractueel vertrouwelijke aangelegenheden. Daarnaast is er geen verwijzing naar de verplichting van de aanvrager om het certificeringsorgaan toegang te verschaffen tot zijn verwerkingsactiviteiten. Het Comité beveelt de Duitse toezichthoudende autoriteiten daarom aan om de voormelde verplichtingen op te nemen in hun ontwerp.

16. Het Comité merkt op dat de expliciete verwijzing naar de taken en bevoegdheden van de bevoegde toezichthoudende autoriteit (deel 4.1.2, punt 3, van de bijlage) niet is opgenomen in deel 4.1.2.2 van het ontwerp van de accreditatie-eisen van de Duitse toezichthoudende autoriteiten. Het Comité is van mening dat deze verwijzing moet worden toegevoegd aan het ontwerp van de eisen en beveelt de Duitse toezichthoudende autoriteiten daarom aan het ontwerp dienovereenkomstig te wijzigen.

17. Bovendien bevat het ontwerp van de eisen van de Duitse toezichthoudende autoriteiten geen verplichting om het certificeringsorgaan toe te staan alle informatie openbaar te maken voor het afgeven van het certificaat overeenkomstig artikel 42, lid 8, en artikel 43, lid 5, AVG (deel 4.1.2, punt 7, van de bijlage). Hoewel die verplichting is opgenomen in het deel over het procesbeheer in het ontwerp van de accreditatie-eisen van de Duitse toezichthoudende autoriteiten, is het Comité van mening dat dit deel moet uitmaken van de certificeringsovereenkomst om zo de bindende aard ervan te versterken. Daarom beveelt het Comité de Duitse toezichthoudende autoriteiten aan om de hiervoor vermelde verplichting op te nemen als een van de elementen van de certificeringsovereenkomst.

18. Op grond van de bijlage moet de aanvrager het certificeringsorgaan op de hoogte stellen van significante veranderingen in zijn feitelijke of juridische situatie en met betrekking tot de producten, processen en diensten waarop de certificering betrekking heeft (deel 4.1.2, punt 10, van de bijlage), In het ontwerp van de accreditatie-eisen van de Duitse toezichthoudende autoriteiten bevat deel 4.1.2.2, punt 6, echter alleen de verplichting om het certificeringsorgaan op de hoogte te stellen van significante veranderingen in zijn feitelijke of juridische situatie, maar worden de producten, processen en diensten niet expliciet genoemd. Het Comité beveelt de Duitse toezichthoudende autoriteiten aan om een dergelijke verwijzing in lijn met de bijlage op te nemen.

19. Met betrekking tot deel 4.2.7 van het ontwerp van de accreditatie-eisen van de Duitse toezichthoudende autoriteiten ("onpartijdigheid van de verwerking") beveelt het Comité aan om de criteria te versterken die van toepassing zijn op certificeringsorganen die onderdeel uitmaken van of worden gecontroleerd door een afzonderlijke juridische entiteit, zodat rekening wordt gehouden met het feit dat eventuele economische relaties tussen het certificeringsorgaan en de juridische entiteit, afhankelijk van hun kenmerken, van invloed kunnen zijn op de onpartijdigheid van zijn certificeringsactiviteiten.

20. Met betrekking tot deel 4.6 van het ontwerp van de accreditatie-eisen van de Duitse toezichthoudende autoriteiten ("openbaar beschikbare informatie") merkt het Comité op dat er geen verwijzing is naar de bekendmaking van alle versies van de goedgekeurde criteria en de certificeringsprocedures. Het Comité spoort de Duitse toezichthoudende autoriteiten daarom aan om

het ontwerp van de accreditatie-eisen zodanig te wijzigen dat er expliciet staat dat de bekendmaking alle versies van de goedgekeurde criteria en de certificeringsprocedures omvat. Daarnaast merkt het Comité op dat in de tweede alinea van deel 4.6 staat dat "de certificeringsregelingen die worden gebruikt door het certificeringsorgaan de goedgekeurde criteria in overeenstemming met artikel 42, lid 5, AVG met vermelding van de toegestane duur van de toepassing, *op algemene wijze moeten worden bekendgemaakt*". Ter voorkoming van dubbelzinnigheid spoort het Comité de Duitse toezichthoudende autoriteiten aan om de woorden "op algemene wijze" te schrappen en om het woord "en" toe te voegen tussen "certificeringsorgaan" en "de goedgekeurde criteria".

2.2.5 EISEN AAN DE MIDDELEN (hoofdstuk 6 van het ontwerp van de accreditatie-eisen)

21. Met betrekking tot de deskundigheidseisen en, meer specifiek, deel 6.1.2.1 van het ontwerp van de accreditatie-eisen van de Duitse toezichthoudende autoriteiten ("bekwaamheden van personele middelen") merkt het Comité op dat de vereiste kennis van de opgesomde gebieden niet specificeert dat de kennis relevant en passend moet zijn. Teneinde de consistentie te waarborgen met het in de bijlage vereiste niveau van deskundigheid, beveelt het Comité de Duitse toezichthoudende autoriteiten aan om de formulering af te stemmen op de richtsnoeren, door te vereisen dat de kennis relevant en passend is.

22. Bovendien merkt het Comité op dat de eisen voor personeel met technische expertise dat verantwoordelijk is voor besluitvorming beschikt over ten minste zeven jaar beroepservaring of vijf jaar beroepservaring op het gebied van technische gegevensbescherming, afhankelijk van hun onderwijsniveau, terwijl het personeel dat verantwoordelijk is voor evaluaties moet beschikken over vier jaar beroepservaring of twee jaar beroepservaring op het gebied van de testprocedure, afhankelijk van hun onderwijsniveau. Personeelsleden met juridische kennis die besluiten nemen, moeten eveneens beschikken over ten minste vijf jaar beroepservaring op het gebied van gegevensbeschermingswetgeving, terwijl diegenen die belast zijn met evaluaties moeten beschikken over ten minste twee jaar ervaring op het gebied van gegevensbeschermingswetgeving en de auditprocedures. Het Comité merkt op dat de vereiste minimale jaren professionele ervaring tussen het personeel dat belast is met de besluitvorming en het personeel dat belast is met de evaluatie aanzienlijk verschillen. Het Comité is in dit opzicht van mening dat de bekwaamheidseisen voor evaluatoren en besluitvormers moet zijn afgestemd op de verschillende taken die zij uitvoeren in plaats van het aantal jaar ervaring. Het Comité is van mening dat evaluatoren meer specialistische kennis en beroepservaring moeten hebben met technische procedures (zoals audits en certificeringen), terwijl besluitvormers moeten beschikken over een meer algemene en uitgebreidere kennis en beroepservaring op het gebied van gegevensbescherming. Het Comité spoort de Duitse toezichthoudende autoriteiten aan dit in overweging te nemen en meer de nadruk te leggen op de verschillende soorten materiële kennis en/of ervaring voor evaluatoren en besluitvormers en de grote verschillen in vereiste jaren ervaring terug te brengen.

23. Daarnaast is het Comité van mening dat de kennis van managementsystemen die relevant zijn voor het certificeringsgebied moet worden uitgebreid tot ISO/IEC 27701:2019 (Veiligheidstechnieken – Uitbreiding op ISO/IEC 27001 en ISO/IEC 27002 voor privacy-informatiemanagement – Eisen en richtlijnen) en spoort de Duitse toezichthoudende autoriteiten aan een dergelijke verwijzing op te nemen.

24. Tot slot is het Comité met betrekking tot onderwijsvereisten voor het technische personeel van mening dat de lijst met onderwerpen reeds is afgestemd op de technische expertise die is vereist in de bijlage. Het Comité spoort de Duitse toezichthoudende autoriteiten daarom aan om de verwijzing naar "natuurwetenschappen" te schrappen van de lijst met onderwerpen betreffende universitaire opleiding van het technisch personeel.

2.2.6 EISEN AAN DE PROCEDURE (hoofdstuk 7 van het ontwerp van de accreditatie-eisen)

25. Het Comité merkt op dat in hoofdstuk 7 van het ontwerp van de accreditatie-eisen van de Duitse toezichthoudende autoriteiten verschillende keren wordt verwezen naar de term "zijn criteria" (bijvoorbeeld in de delen 7.4, 7.6, 7.11 en 7.13). Teneinde dubbelzinnigheid te voorkomen, spoort het Comité de Duitse toezichthoudende autoriteiten aan om de betekenis van die term te verduidelijken, bijvoorbeeld door een toelichting op te nemen in aanhangsel 1 (Woordenlijst).

26. Met betrekking tot deel 7.1 van het ontwerp van de accreditatie-eisen van de Duitse toezichthoudende autoriteiten ("algemene informatie") merkt het Comité op dat er niet expliciet wordt verwezen naar de verplichting van het certificeringsorgaan om te voldoen aan de aanvullende eisen. Hoewel een dergelijke verplichting kan worden afgeleid uit de tekst van het ontwerp van de eisen, is het Comité van mening dat een expliciete verwijzing naar de hiervoor vermelde verplichting moet worden opgenomen. Het Comité beveelt de Duitse toezichthoudende autoriteiten derhalve aan om het ontwerp dienovereenkomstig te wijzigen.

27. Het Comité merkt op dat het ontwerp van de aanvullende eisen van de Duitse toezichthoudende autoriteiten geen verwijzing bevatten naar de werking van een goedgekeurd Europees gegevensbeschermingszegel, overeenkomstig deel 7.1.2 van de bijlage. Het Comité is van mening dat deze verwijzing moet worden opgenomen, vooral gezien het feit dat de accreditatie van een certificeringsorgaan dat Europese gegevensbeschermingszegels uitgeeft, mogelijk moet worden uitgevoerd in elk van de lidstaten waar het certificeringsorgaan is gevestigd.[3] Het Comité beveelt de Duitse toezichthoudende autoriteiten derhalve aan om de hiervoor vermelde verwijzing op te nemen. In het ontwerp van de eisen kan bijvoorbeeld het volgende worden vermeld: *"De bevoegde toezichthoudende autoriteit wordt ingelicht voordat een certificeringsorgaan in een nieuwe lidstaat vanuit een bijkantoor begint te werken met een goedgekeurd Europees gegevensbeschermingszegel."*

28. Het Comité merkt op dat in deel 7.2 ("aanvraag") van het ontwerp van de accreditatie-eisen van de Duitse toezichthoudende autoriteiten is voorzien in de situatie waarin verwerkers worden ingezet om gegevensverwerkingsactiviteiten uit te voeren, in overeenstemming met de bijlage bij de richtsnoeren. Het Comité merkt echter op dat wanneer er gebruik wordt gemaakt van verwerkers, bij de aanvraag de overeenkomst(en) van de betreffende verwerkingsverantwoordelijke/verwerker moet(en) worden gevoegd, zoals vermeld in de bijlage. Het Comité beveelt de Duitse toezichthoudende autoriteiten daarom aan om de formulering in overeenstemming te brengen met de richtsnoeren door de verwijzing naar de overeenkomst(en) van de verwerkingsverantwoordelijke/verwerker op te nemen. Bovendien spoort het Comité de Duitse toezichthoudende autoriteiten aan om te overwegen in dit geval ook een verwijzing te maken naar gezamenlijke verwerkingsverantwoordelijken en hun specifieke regelingen.

[3] Zie in dit verband richtsnoeren 1/2018, punt 44.

29. Het Comité merkt op dat in deel 7.2 van het ontwerp van de accreditatie-eisen van de Duitse toezichthoudende autoriteiten wordt gespecificeerd dat “de verwerkingsverantwoordelijke en de verwerker certificering kunnen aanvragen”. De mogelijkheid voor verwerkers om een certificeringsaanvraag in te dienen, is afhankelijk van de specifieke certificeringsregeling. Het Comité spoort de Duitse toezichthoudende autoriteiten daarom ter voorkoming van verwarring aan om de bovenstaande verwijzing te schrappen of om te verduidelijken dat de mogelijkheid voor verwerkers om te worden gecertificeerd, afhankelijk is van het toepassingsgebied van de certificeringsregeling.

30. Met betrekking tot deel 7.3 van het ontwerp van de accreditatie-eisen van de Duitse toezichthoudende autoriteiten (“evaluatieaanvragen”) merkt het Comité op dat in het ontwerp van de accreditatie-eisen van de Duitse toezichthoudende autoriteiten staat dat “de geplande evaluatiemethoden contractueel zijn voorgeschreven [...]”. Om duidelijk te maken dat dit een eis is, spoort het Comité de Duitse toezichthoudende autoriteiten aan om de eerste alinea opnieuw te formuleren om duidelijk te maken dat de evaluatiemethoden worden opgenomen in de certificeringsovereenkomst. Dit houdt in dat de eis als volgt opnieuw wordt geformuleerd: “de geplande evaluatiemethoden worden contractueel voorgeschreven [...]”. Daarnaast spoort het Comité de Duitse toezichthoudende autoriteiten aan om de verwijzing naar punt 7.3.1.b van ISO 17065 te vervangen door punt 7.3 van ISO 17065, om de formulering zo in overeenstemming te brengen met de bijlage. Bovendien merkt het Comité op dat in de vierde alinea wordt verwezen naar de passende technische en juridische bekwaamheden. Het Comité spoort de Duitse toezichthoudende autoriteiten aan om voor de duidelijkheid “op het gebied van gegevensbescherming” toe te voegen.

31. Het Comité merkt op dat deel 7.4 van het ontwerp van de accreditatie-eisen van de Duitse toezichthoudende autoriteiten (“evaluatiemethoden”) niet de verplichting van het certificeringsorgaan bevat om evaluatiemethoden te beschrijven die toereikend zijn om te beoordelen of de verwerkingsactiviteiten voldoen aan de certificeringscriteria. Daarom raadt het Comité de Duitse toezichthoudende autoriteiten aan om het ontwerp van de eisen aan te passen en een dergelijke verwijzing op te nemen. Er kan bijvoorbeeld het volgende worden toegevoegd: *“Het certificeringsorgaan zorgt ervoor dat mechanismen die worden gebruikt voor de uitgifte van de certificering toereikende evaluatiemethoden beschrijven voor de beoordeling of de verwerkingsactiviteiten voldoen aan de certificeringscriteria.”* Bovendien is het Comité met betrekking tot het eerste gebied waarop de evaluatiemethoden van toepassing zullen zijn van mening dat de noodzaak en evenredigheid ook worden beoordeeld in verband met de desbetreffende betrokkenen, indien van toepassing. Tot slot merkt het Comité op dat er geen verwijzing wordt gemaakt naar de documentatie van methoden en bevindingen. Daarom spoort het Comité de Duitse toezichthoudende autoriteiten aan om het ontwerp aan te passen en een dergelijke verwijzing expliciet op te nemen.

32. Met betrekking tot bestaande certificeringen (deel 7.4 van het ontwerp van de accreditatie-eisen van de Duitse toezichthoudende autoriteiten) is het Comité van mening dat het vierde streepje op pagina 13 tot verwarring leidt, aangezien niet duidelijk is wat het verband is tussen de geldigheidsperioden van huidige en eerdere certificering en hoe deze op elkaar aansluiten. Daarnaast lijkt het niet haalbaar om de geldigheid van eerdere door een ander certificeringsorgaan afgegeven certificering in twijfel te trekken. Deze alinea zou derhalve baat hebben bij enige verduidelijking ten aanzien van de relatie tussen de verschillende vermelde elementen. Het Comité beveelt de Duitse toezichthoudende autoriteiten aan om het ontwerp met name aan te passen door te verduidelijken dat de geldigheid van andere soorten certificeringen geen voorwaarde mag zijn voor de duur van de geldigheid van de AVG-certificering.

33. Met betrekking tot deel 7.5 (“waardering”) van het ontwerp van de accreditatie-eisen van de Duitse toezichthoudende autoriteiten spoort het Comité de Duitse toezichthoudende autoriteiten aan de titel van het deel te wijzigen in “beoordeling”.

34. Met betrekking tot wijzigingen die van invloed zijn op de certificering (deel 7.10 van het ontwerp van de accreditatie-eisen van de Duitse toezichthoudende autoriteiten) merkt het Comité op dat in het ontwerp van de accreditatie-eisen van de Duitse toezichthoudende autoriteiten wordt vastgesteld dat “de klant tijdig wordt geïnformeerd over wijzigingen in het rechtskader die op hem van invloed zijn”. In gedachten houdend dat de onpartijdigheid van het certificeringsorgaan in stand moet worden gehouden, spoort het Comité de Duitse toezichthoudende autoriteiten aan om die zin opnieuw te formuleren om duidelijk te maken dat de klant tijdig algemene informatie ontvangt over wijzigingen die op hem van invloed kunnen zijn. Om tevens te waarborgen dat duidelijk wordt begrepen wat wordt verstaan onder “besluiten van het Europees Comité voor gegevensbescherming” spoort het Comité de Duitse toezichthoudende autoriteiten aan de verwijzing te verduidelijken. Een voorbeeld zou kunnen zijn om te verwijzen naar “door het Europees Comité voor gegevensbescherming vastgestelde documenten”.

35. Het Comité merkt op dat deel 7.11 van het ontwerp van de accreditatie-eisen van de Duitse toezichthoudende autoriteiten (“beëindiging, beperking, opschorting of intrekking van de certificering”) geen verplichting bevat om besluiten en opdrachten van de Duitse toezichthoudende autoriteiten te aanvaarden om de certificering in te trekken of niet af te geven aan een aanvrager indien niet langer wordt voldaan aan de certificeringseisen. Het Comité beveelt de Duitse toezichthoudende autoriteiten derhalve aan om een dergelijke verplichting op te nemen. Daarnaast spoort het Comité de Duitse toezichthoudende autoriteiten aan om, in overeenstemming met de bijlage bij de richtsnoeren, in de titel van dit deel het woord “beperking” te vervangen door “vermindering”.

2.2.7 VERDERE AANVULLENDE EISEN

36. Met betrekking tot deel 8.11.3 van de accreditatie-eisen van de Duitse toezichthoudende autoriteiten (“beheer van klachten”) spoort het Comité de Duitse toezichthoudende autoriteiten aan om de verwijzing naar “gerechtvaardigde klachten” te vervangen door “gemotiveerde klachten” om zo meer duidelijkheid te bieden.

3 CONCLUSIES/AANBEVELINGEN

37. Het ontwerp van de accreditatie-eisen van de Duitse toezichthoudende autoriteiten van de Federatie en de Länder kan leiden tot een incoherente toepassing van de accreditatie van certificeringsorganen. De volgende wijzigingen moeten worden aangebracht:

38. Ten aanzien van de “algemene opmerkingen” beveelt het Comité aan dat de Duitse toezichthoudende autoriteiten:

    1) de verwijzing naar “toestemming door het EDPB” schrappen om ervoor te zorgen dat het ontwerp overeenstemt met de formulering in de AVG.

39. Ten aanzien van de “algemene eisen voor accreditatie” beveelt het Comité aan dat de Duitse toezichthoudende autoriteiten:

1) de eisen betreffende de wettelijke verantwoordelijkheid (deel 4.1) aanpassen om deze in lijn te brengen met de richtsnoeren;

2) deel 4.1.2.2 aanpassen om in de certificeringsovereenkomst de verplichting op te nemen om volledige transparantie mogelijk te maken voor de Duitse toezichthoudende autoriteiten met betrekking tot de certificeringsprocedure en om het certificeringsorgaan toegang te verschaffen tot de verwerkingsactiviteiten van de aanvrager;

3) in deel 4.1.2.2 een expliciete verwijzing opnemen naar de taken en bevoegdheden van de bevoegde toezichthoudende autoriteit, in overeenstemming met de bijlage;

4) in de elementen van de certificeringsovereenkomst de verplichting opnemen om het certificeringsorgaan toe te staan alle informatie openbaar te maken voor het afgeven van het certificaat overeenkomstig artikel 42, lid 8, en artikel 43, lid 5, AVG;

5) in deel 4.1.2.2, punt 6, een expliciete verwijzing opnemen naar de "producten, processen en diensten waarop de certificering betrekking heeft";

6) in deel 4.2.7 de criteria versterken die van toepassing zijn op certificeringsorganen die onderdeel uitmaken van of worden gecontroleerd door een afzonderlijke juridische entiteit, zodat rekening wordt gehouden met het feit dat eventuele economische relaties tussen het certificeringsorgaan en de juridische entiteit, afhankelijk van zijn kenmerken, van invloed kunnen zijn op de onpartijdigheid van zijn certificeringsactiviteiten.

40. Ten aanzien van de "eisen aan middelen" beveelt het Comité aan dat de Duitse toezichthoudende autoriteiten:

1) de formulering van deel 6.1.2.1 in lijn brengen met de richtsnoeren, door te vereisen dat de kennis relevant en passend is.

41. Ten aanzien van de "eisen aan de procedure" beveelt het Comité aan dat de Duitse toezichthoudende autoriteiten:

1) deel 7.1 aanpassen zodat deze een expliciete verwijzing bevat naar de verplichting van het certificeringsorgaan om te voldoen aan de aanvullende eisen;

2) een verwijzing opnemen naar de werking van een goedgekeurde Europese gegevensbeschermingszegel;

3) de formulering van deel 7.2 afstemmen op de richtsnoeren door een verwijzing op te nemen naar de overeenkomst(en) van de verwerkingsverantwoordelijke/verwerker;

4) in deel 7.4 de verplichting opnemen van het certificeringsorgaan om toereikende evaluatiemethoden te beschrijven om de naleving te beoordelen van de verwerkingsactiviteit(en) met de certificeringscriteria;

5) in deel 7.4 verduidelijken dat de geldigheid van andere soorten certificeringen geen voorwaarde mag zijn voor de duur van de geldigheid van de AVG-certificering;

6) in deel 7.11 de verplichting opnemen om besluiten en opdrachten van de Duitse toezichthoudende autoriteiten te aanvaarden om de certificering in te trekken of niet af te geven aan een aanvrager indien niet langer wordt voldaan aan de certificeringseisen.

4 SLOTOPMERKINGEN

42. Dit advies is gericht tot de Duitse toezichthoudende autoriteiten van de Federatie en de Länder en wordt bekendgemaakt op grond van artikel 64, lid 5, onder b), AVG.

43. Overeenkomstig artikel 64, leden 7 en 8, AVG delen de Duitse toezichthoudende autoriteiten de voorzitter binnen twee weken na ontvangst van het advies langs elektronische weg mee of zij hun ontwerpbesluit zullen wijzigen dan wel handhaven. Binnen dezelfde termijn verstrekken zij het gewijzigde ontwerpbesluit of, indien zij niet van plan zijn het advies van het Comité op te volgen, geven zij de redenen op waarom zij voornemens zijn het advies geheel of gedeeltelijk niet op te volgen.

44. De Duitse toezichthoudende autoriteiten zullen het uiteindelijke besluit aan het Comité meedelen zodat het overeenkomstig artikel 70, lid 1, onder y), AVG kan worden opgenomen in het register van besluiten die onderworpen zijn aan het coherentiemechanisme.

Voor het Europees Comité voor gegevensbescherming

De voorzitter

(Andrea Jelinek)

Vastgesteld