Advies van de EDPB (artikel 64)

# Advies 14/2020 over het ontwerpbesluit van de bevoegde toezichthoudende autoriteit van Ierland betreffende de goedkeuring van de accreditatie-eisen van een certificeringsorgaan overeenkomstig artikel 43, lid 3 van de 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), 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: "de 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 om te zorgen voor een consequente toepassing van de AVG binnen 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 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 Richtsnoeren 4/2018 van het EDPB inzake de accreditatie van certificeringsorganen 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 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.

4) De "Richtsnoeren 4/2018 betreffende de accreditatie van certificeringsorganen volgens artikel 43 van de algemene verordening gegevensbescherming (2016/679)" (hierna: "de richtsnoeren") en de "Richtsnoeren 1/2018 betreffende certificering en het identificeren van

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

certificeringscriteria in overeenstemming met 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, 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 van de AVG betreffende de eisen voor accreditatie, die van toepassing zijn wanneer de toezichthoudende autoriteit zelf de accreditatie verzorgt, 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 dient ISO/IEC 17065 een leidraad te zijn voor de door de toezichthoudende autoriteit gehanteerde accreditatie-eisen en dienen deze te worden aangevuld met de aanvullende eisen die een toezichthoudende autoriteit vaststelt op grond van artikel 43, lid 1, onder b) van de AVG. Het EDPB merkt op dat artikel 43, lid 2, onder a) tot en met e) van de AVG 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 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 Ierland (hierna: "Ierse toezichthouder") heeft haar 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 Ierland (INAB) voert de accreditatie van certificeringsorganen om te certificeren uit met behulp van de certificeringscriteria in de AVG. Dit houdt in dat de INAB gebruik zal maken van ISO 17065 en de aanvullende eisen die zijn voorgeschreven door de Ierse toezichthouder, nadat deze door de Ierse toezichthouder zijn vastgesteld na een advies van het Comité over de ontwerpeisen, voor de accreditatie van certificeringsorganen.

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 inzake 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_en

# 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 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 Ierse toezichthouder heeft besloten de uitgifte van accreditaties onder te brengen bij zijn nationale accreditatie-instantie. De Ierse toezichthouder heeft aanvullende eisen opgesteld in overeenstemming met de richtsnoeren die door de nationale accreditatie-instantie moeten worden gebruikt bij de uitgifte van accreditaties.

4. Deze beoordeling van de aanvullende accreditatie-eisen van de Ierse toezichthouder is gericht op het onderzoek van variaties (toevoegingen of schrappingen) op de richtsnoeren en met name bijlage 1. 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 autoriteit op een manier die de praktische en coherente toepassing ervan mogelijk maakt, zoals vereist in de context van de toezichthoudende autoriteit.

6. 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.

7. 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 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 Ierse toezichthouder niet aan bod komt, houdt dit in dat het Comité geen opmerkingen heeft en de Ierse toezichthouder niet verzoekt om nadere actie te ondernemen.

9. Dit advies gaat niet in op door de Ierse toezichthouder ingediende zaken 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:

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 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 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 PREFIX (deel 0 van het ontwerp van de accreditatie-eisen van de Ierse toezichthouder)

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 de verwijzing naar de richtsnoeren inzake accreditatie als “WP 261” niet is bijgewerkt. Het EDPB heeft de Richtsnoeren 4/2018 inzake de accreditatie van certificeringsinstanties op grond van artikel 43 van de algemene verordening gegevensbescherming (2016/679) vastgesteld. Daarom spoort het Comité de Ierse toezichthouder aan om de formulering aan te passen en te verwijzen naar de Richtsnoeren 4/2018.

### 2.2.3 ALGEMENE OPMERKINGEN

13. Het Comité merkt op dat de ontwerpeisen van de Ierse toezichthouder herhaaldelijk verwijzen naar de “bevoegde toezichthoudende autoriteit”. Aangezien de Ierse toezichthouder in dit geval de bevoegde toezichthoudende autoriteit is, spoort het Comité de Ierse toezichthouder aan om de verwijzing te vervangen door “de DPC” of “de Ierse toezichthouder” om verwarring te voorkomen.

14. Het Comité erkent dat de ontwerpeisen van de Ierse toezichthouder een sectie bevatten over termen en definities. Sommige termen worden echter niet op consistente wijze gebruikt in het document (zoals “onderwerp van beoordeling” en “ToE”). Het Comité spoort de Ierse toezichthouder dan ook aan consistente terminologie te gebruiken in de ontwerpeisen om zo verwarring te voorkomen.

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

15. Met betrekking tot punt 7 van artikel 4.1.2 van het ontwerp van de accreditatie-eisen van de Ierse toezichthouder is het Comité van mening dat de formulering enigszins onduidelijk is met betrekking tot degene aan wie de redenen voor de goedkeuring van de certificering worden verstrekt. Bovendien is de verwijzing naar de “facilitering” van het register ook onduidelijk. Het Comité spoort de Ierse toezichthouder daarom aan om dit punt opnieuw te formuleren op een manier die meer duidelijkheid verschaft.

### 2.2.5 EISEN AAN DE STRUCTUUR (deel 5 van het ontwerp van de accreditatie-eisen)

16. Het Comité merkt op dat het ontwerp van de accreditatie-vereisten van de Ierse toezichthouder verwijst naar de benoeming van “een persoon met de relevante anciënniteit met verantwoordelijkheid voor het toezicht op de naleving van gegevensbescherming en informatiegovernance”. De verwijzing naar de relevante anciënniteit moet worden verduidelijkt in de zin van ervaring en toepassingsgebied van de autoriteit. Bovendien lijken de functies van deze persoon op die van de functionaris voor gegevensbescherming. Het Comité spoort de Ierse toezichthouder aan om de functies van deze persoon duidelijk vast te stellen en de relevante ervaring te specificeren.

### 2.2.6 EISEN AAN DE MIDDELEN (deel 6 van het ontwerp van de accreditatie-eisen)

17. Met betrekking tot het personeel van het certificeringsorgaan (artikel 6.1) merkt het Comité op dat de eisen aan personeel met technische kennis verantwoordelijk voor de besluitvorming onder meer bestaan uit ten minste vijf jaar professionele ervaring die verband houdt met het onderwerp van de certificering, terwijl het personeel dat verantwoordelijk is voor evaluaties moet beschikken over ten minste twee jaar professionele ervaring. Personeelsleden met juridische kennis die besluiten nemen moeten eveneens beschikken over vijf jaar professionele ervaring, terwijl diegenen die belast zijn met evaluaties moeten beschikken over ten minste twee jaar ervaring. 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 verband van mening dat de nadruk moet liggen op het verschillende soort deskundigheid en niet op het aantal jaren professionele ervaring. 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. Het Comité spoort de Ierse toezichthouder 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.

### 2.2.7 EISEN AAN DE PROCEDURE (deel 7 van het ontwerp van de accreditatie-eisen)

18. Met betrekking tot artikel 7.10 van het ontwerp van de accreditatie-eisen van de Ierse toezichthouder (“Wijzigingen die van invloed zijn op de certificering”) merkt het Comité op dat er niet wordt verwezen naar de overeen te komen wijzigingsprocedures overeenkomstig artikel 7.10 van de bijlage. Het Comité spoort de Ierse toezichthouder aan om een dergelijke verwijzing op te nemen en enkele van de mogelijk in te voeren procedures (zoals overgangsperiodes, goedkeuringsprocedure bij de bevoegde toezichthoudende autoriteit, enz.) te vermelden. Daarnaast is het Comité van mening dat wijzigingen in de technologische ontwikkeling ook relevant zijn en van invloed kunnen zijn op de certificering. Daarom spoort het Comité de Ierse toezichthouder aan om deze mogelijkheid op te nemen in de lijst van wijzigingen die van invloed zijn op de certificering. Tot slot is het Comité ingenomen met de opname van inbreuken in verband met persoonsgegevens en schendingen van de AVG op de lijst met wijzigingen die van invloed kunnen zijn op de certificering. Om de duidelijkheid te verzekeren spoort het Comité de Ierse toezichthouder echter aan om te specificeren dat met de inbreuken in verband met persoonsgegevens of de schendingen van de AVG alleen rekening wordt gehouden voor zover ze verband houden met de certificering.

19. Met betrekking tot de wijzigingen die van invloed zijn op de certificering (artikel 7.10 van het ontwerp van de accreditatie-eisen van de Ierse toezichthouder) en, met name, het vijfde opsommingsteken merkt het Comité op dat de Ierse toezichthouder verwijst naar “toepasselijke bindende besluiten van het Europees Comité voor gegevensbescherming” en tevens naar artikel 39 van het reglement van orde van het Comité, die “alle definitief door het Comité vastgestelde documenten” omvat. Teneinde te waarborgen dat duidelijk wordt begrepen wat wordt verstaan onder “besluiten van het Europees Comité voor gegevensbescherming” spoort het Comité de Ierse toezichthouder aan de verwijzing te verduidelijken. Een voorbeeld zou kunnen zijn om te verwijzen naar “door het Europees Comité voor gegevensbescherming vastgestelde documenten”.

20. Het Comité merkt op dat artikel 7.11 van het ontwerp van de accreditatie-eisen van de Ierse toezichthouder ("Beëindiging, beperking, opschorting of intrekking van de certificering") geen verplichting bevat om besluiten en opdrachten van de Ierse toezichthouder 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 Ierse toezichthouder aan om een dergelijke verplichting op te nemen.

# 3 CONCLUSIES/AANBEVELINGEN

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

22. Ten aanzien van de 'eisen aan de procedure' beveelt het Comité aan dat de Ierse toezichthouder:

1) in artikel 7.11 de verplichting opneemt om besluiten en opdrachten van de Ierse toezichthouder 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

23. Dit advies is gericht tot de Ierse toezichthouder en wordt bekendgemaakt op grond van artikel 64, lid 5, onder b) van de AVG.

24. Overeenkomstig artikel 64, leden 7 en 8 van de AVG deelt de Ierse toezichthouder 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 van plan 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.

25. De Ierse toezichthouder zal het uiteindelijke besluit aan het Comité meedelen zodat het overeenkomstig artikel 70, lid 1, onder y) van de 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)