

Advies van de EDPB (artikel 64)



Advies 16/2020 over het ontwerpbesluit van de bevoegde toezichthoudende autoriteit van Tsjechië betreffende de goedkeuring van de accreditatie-eisen van een certificeringsorgaan krachtens artikel 43, lid 3 (AVG)

Vastgesteld op 25 mei 2020

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

Inhoudsopgave

1	SAMENVATTING VAN DE FEITEN.....	4
2	BEOORDELING	5
2.1	Algemene redenering van het EDPB met betrekking tot het ingediende ontwerpbesluit.....	5
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:	6
2.2.1	VOORBEPALING.....	7
2.2.2	ALGEMENE OPMERKINGEN	7
2.2.3	ALGEMENE EISEN VOOR ACCREDITATIE	7
2.2.4	EISEN AAN DE MIDDELEN	9
2.2.5	EISEN AAN DE PROCEDURE.....	9
2.2.6	BEHEERSYSTEEM	11
3	CONCLUSIES/AANBEVELINGEN	11
4	SLOTOPMERKINGEN.....	13

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 2018¹,

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 consistente toepassing van Verordening (EU) 2016/679 (hierna: “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, is zij er wel op gericht coherentie te bevorderen. Het Comité streeft ernaar deze doelstelling te bereiken in zijn adviezen door ten eerste toezichthoudende autoriteiten aan te moedigen hun eisen voor accreditatie op te stellen overeenkomstig de structuur die is uiteengezet in de bijlage bij de richtsnoeren van het EDPB inzake de accreditatie van certificeringsorganen en, ten tweede, deze te analyseren met behulp van een door het EDPB verstrekt sjabloon waarmee de eisen kunnen worden gebenchmarkt (op basis van ISO 17065 en de richtsnoeren van het EDPB inzake de accreditatie van certificeringsorganen).

(2) Onder verwijzing naar artikel 43 van de AVG stellen de bevoegde toezichthoudende autoriteiten accreditatie-eisen vast. Ze passen hierbij echter het coherentiemechanisme toe om ervoor te zorgen dat er vertrouwen wordt gesteld 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 betreffende de accreditatie van certificeringsorganen volgens artikel 43 van de algemene verordening gegevensbescherming (2016/679)” (hierna: “de richtsnoeren” genoemd) en de “Richtsnoeren 1/2018 betreffende certificering en het identificeren van 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, moet de toezichthoudende autoriteit accreditatie-eisen vaststellen, die onder meer ook de in artikel 43, lid 2, vermelde eisen omvatten. In vergelijking met de plichten in verband met de accreditatie van certificeringsorganen door nationale accreditatie-instanties bevat artikel 43 minder details ten aanzien van de eisen voor accreditatie wanneer de toezichthoudende autoriteit zelf de accreditatie ter hand neemt. 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, 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 Tsjechië (hierna: “Tsjechische toezichthouder” genoemd) heeft haar ontwerp van de accreditatie-eisen krachtens artikel 43, lid 1, onder b), ingediend bij het EDPB. Het dossier is op 17 februari 2020 als volledig aangemerkt. De nationale accreditatie-instantie van Tsjechië voert de accreditatie van certificeringsorganen om te certificeren uit met behulp van de certificeringscriteria in de AVG. Dit houdt in dat de nationale accreditatie-instantie gebruik zal maken van ISO 17065 en de aanvullende eisen die zijn voorgeschreven door de toezichthoudende autoriteit van Tsjechië, nadat deze door de toezichthoudende autoriteit zijn vastgesteld na een advies van het Comité over de ontwerp-eisen, 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 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/retningslijnjer/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 Tsjechische toezichthouder heeft besloten de uitgifte van accreditaties onder te brengen bij zijn nationale accreditatie-instantie. De Tsjechische 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 Tsjechische 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 punten 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: "de bijlage"). Indien in dit advies een specifiek deel van het ontwerp van de accreditatie-eisen van de Tsjechische toezichthouder niet aan bod komt, houdt dit in dat het Comité geen opmerkingen heeft en de Tsjechische toezichthouder niet verzoekt om nadere actie te ondernemen.
9. Dit advies gaat niet in op door de Tsjechische 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:

- 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. belangenverstremgeling 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.

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 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 ALGEMENE OPMERKINGEN

12. Het Comité merkt op dat het ontwerp van de accreditatie-eisen de in bijlage 1 bij de richtsnoeren weergegeven indeling niet volledig volgt. De delen over “toepassingsgebied” en “termen en definities” ontbreken bijvoorbeeld. Ten behoeve van de duidelijkheid en om een gemakkelijker beoordeling van de eisen mogelijk te maken, is het Comité van mening dat de nummering en de algemene indeling van het document voor verbetering vatbaar zijn. Om de beoordeling te vergemakkelijken moedigt het Comité de Tsjechische toezichthouder dan ook aan om in de ontwerpeisen de structuur van de bijlage te volgen en de ontbrekende delen toe te voegen, waarbij vooral de definities van de termen die in het document worden gebruikt, van belang zijn. Het Comité merkt bovendien op dat in het ontwerp van de accreditatie-eisen van de Tsjechische toezichthouder meermaals wordt verwezen naar het overeenkomstige deel van ISO 17065 of de overeenkomstige delen van de bijlage, zonder dat deze verwijzingen worden gespecificeerd. Het Comité spoort de Tsjechische toezichthouder daarom aan om de verwijzingen naar de delen van ISO 17065 en de bijlage te verduidelijken.
13. Het Comité merkt op dat in het ontwerp van de accreditatie-eisen van de Tsjechische toezichthouder herhaaldelijk wordt verwezen naar het “beoordeelde voorwerp” (bv. de delen 3.2.1.2.1.2.10; 3.2.1.2.6.3.1; 3.2.1.2.8.1.6.3; 3.2.1.2.10.4.1; 3.1.2.10.7.3.1; 3.1.2.10.7.3.2 en 3.2.1.2.10.10.2). Het Comité begrijpt dat deze term wordt gebruikt als synoniem voor “onderwerp van beoordeling”. Ten behoeve van de duidelijkheid moedigt het Comité de Tsjechische toezichthouder aan om consequent de term “onderwerp van beoordeling” te gebruiken.
14. Het Comité merkt op dat meerdere eisen niet als verplichting van het certificeringsorgaan zijn geformuleerd (bv. 3.2.1.2.2 en 3.2.1.2.3). Het Comité spoort de Tsjechische toezichthouder aan om de eisen te herformuleren en duidelijk te maken dat ze verplicht zijn, d.w.z. om de eis te beginnen met “Het certificeringsorgaan moet [...]”.

2.2.3 ALGEMENE EISEN VOOR ACCREDITATIE

15. Wat betreft de certificeringsovereenkomst (deel 3.2.1.2.1.2 van het ontwerp van de accreditatie-eisen van de Tsjechische toezichthouder) merkt het Comité op dat deel 3.2.1.2.1.2.2 geen enkele verwijzing bevat naar de “contractueel vertrouwelijke aangelegenheden” waartoe de toezichthoudende autoriteit ook toegang moet hebben. Daarom beveelt de Comité de Tsjechische toezichthouder aan om het ontwerp te wijzigen en er ook de verplichting in op te nemen om de toezichthoudende autoriteit toegang te verlenen tot contractueel vertrouwelijke aangelegenheden.
16. Wat betreft deel 3.2.1.2.1.2.8 van het ontwerp van de accreditatie-eisen van de Tsjechische toezichthouder merkt het Comité op dat het onduidelijk is aan wie de informatie openbaar moet worden gemaakt. Daarom moedigt het Comité de Tsjechische toezichthouder aan om de ontvanger

van de informatie te specificeren. Bovendien moet de bedoelde informatie “nodig [zijn] voor het afgeven van het certificaat”, zoals bepaald in punt 4.1.2, item 7, van de bijlage. Het Comité beveelt de Tsjechische toezichthouder aan om “informatie voor het afgeven van het certificaat” te vervangen door “informatie die nodig is voor het afgeven van het certificaat”.

17. Wat betreft deel 3.2.1.2.1.2.9 van de het ontwerp van de accreditatie-eisen van de Tsjechische toezichthouder is het onduidelijk welk soort informatie rechtstreeks aan het Comité moet worden verstrekt. Artikel 42, lid 8, van de AVG verplicht het Comité ertoe om, onder andere, alle certificeringsmechanismen te verzamelen. In dit verband wordt aangenomen dat de bevoegde toezichthouders de betreffende informatie aan het Comité zullen verstrekken, dat deze vervolgens in het openbaar register zal publiceren. Daarom beveelt het Comité de Tsjechische toezichthouder aan om deel 3.2.1.2.1.2.9 van de ontwerp-eisen te verduidelijken in overeenstemming met artikel 42, lid 8, van de AVG.
18. Wat betreft deel 3.2.1.2.1.2.12 van het ontwerp van de accreditatie-eisen van de Tsjechische toezichthouder neemt het Comité er nota van dat de Tsjechische toezichthouder een geherformuleerde versie van een deel van de in de bijlage opgenomen eis heeft opgesteld. De Tsjechische toezichthouder heeft echter een verwijzing achterwege gelaten naar de bepaling dat [indien van toepassing] “ook rekening moet worden gehouden met alle gevolgen voor diens klanten”. Het Comité beveelt de Tsjechische toezichthouder dan ook aan om het ontbrekende gedeelte van voornoemde eis toe te voegen.
19. Daarnaast is in deel 3.2.1.2.1.2.13 van het ontwerp van de accreditatie-eisen van de Tsjechische toezichthouder de verplichting opgenomen om “een toezegging van de aanvrager te bevatten om het certificeringsorgaan op de hoogte te stellen van alle veranderingen die van invloed kunnen zijn op de conformiteit van het gecertificeerde voorwerp met de certificeringscriteria”. Het Comité is acht deze formulering te algemeen en beveelt de Tsjechische toezichthouder aan de ontwerp-eisen te wijzigen met de toevoeging “alle veranderingen in zijn feitelijke of juridische situatie en met betrekking tot de producten, processen en diensten waarop de certificering betrekking heeft”.
20. Wat betreft het gebruik van gegevensbeschermingszegels en -merktekens (deel 3.2.1.2.1.3 van het ontwerp van de accreditatie-eisen van de Tsjechische toezichthouder) merkt het Comité op dat in de ontwerp-eisen van de Tsjechische toezichthouder staat dat de certificeringsovereenkomst “regels voor het gebruik van certificaten, zegels en merktekens moet bevatten indien deze door de eigenaar van de certificeringsregeling zijn verstrekt”. Dezelfde formulering is te vinden in deel 3.2.1.2.1.2.14. Het Comité is van oordeel dat deze verplichting al onder punt 4.1.2.2, onder I), van ISO 17065 valt en daarom in elke certificeringsregeling moet worden opgenomen (zie ook punt 4.1.3 van ISO 17065). Ten behoeve van de duidelijkheid beveelt het Comité de Tsjechische toezichthouder dan ook aan de bovengenoemde delen te schrappen.
21. Wat betreft de eisen inzake onpartijdigheidsmanagement, zijn volgens de informatie die de Tsjechische toezichthouder heeft verstrekt in het ontwerp, punt 4.2.1, letter b), en punt 4.2.2 van de bijlage, voldoende geregeld in punt 4.2 van ISO 17065. Het Comité is echter van mening dat deze eisen expliciet moeten worden opgenomen in het ontwerp van de accreditatie-eisen die door de toezichthoudende autoriteiten overeenkomstig de bijlage worden opgesteld. Daarom beveelt het Comité de Tsjechische toezichthouder aan om de ontbrekende eisen met betrekking tot het onpartijdigheidsmanagement over te nemen uit de bijlage.

22. Wat betreft de eis inzake aansprakelijkheid en financiering (deel 3.2.1.2.3.1 van de ontwerp-eisen van de Tsjechische toezichthouder) moedigt het Comité de Tsjechische toezichthouder aan om te specificeren dat een en ander op regelmatige basis moet worden gewaarborgd.

2.2.4 EISEN AAN DE MIDDELEN

23. Wat betreft het personeel van het certificeringsorgaan (deel 3.2.1.2.8.1.6 van het ontwerp van de accreditatie-eisen van de Tsjechische toezichthouder) merkt het Comité op dat de eisen voor personeelsleden die verantwoordelijk zijn voor evaluaties (deel 3.2.1.2.8.1.6.3) *“vijf jaar praktijkervaring omvatten waarin ten minste tien audits zijn uitgevoerd in het kader van certificeringsactiviteiten op hetzelfde of een soortgelijk gebied [...] of vijf jaar praktijkervaring in het kader van de certificering van de voorwerpen waar het certificeringsorgaan zich op richt”*. Evenzo omvatten de eisen voor personeelsleden die verantwoordelijk zijn voor de besluitvorming (deel 3.2.1.2.8.1.6.4) *“ten minste vijf jaar praktijkervaring waarin ten minste tien audits zijn uitgevoerd in het kader van certificeringsactiviteiten op hetzelfde of een soortgelijk gebied”*. Het Comité is van mening dat de deskundigheidseisen voor evaluatoren en besluitvormers moeten worden afgestemd op de verschillende taken die zij uitvoeren. In dit verband is het Comité 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. In dit licht moedigt het Comité de Tsjechische 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.
24. Voorts neemt het Comité er nota van dat in deel 3.2.1.2.9.1 van het ontwerp van de accreditatie-eisen van de Tsjechische toezichthouder wordt bepaald dat uitbesteding voor certificeringsactiviteiten niet is toegestaan. Het volgende punt biedt evenwel de mogelijkheid om voor de evaluatie gebruik te maken van externe auditors en externe deskundigen, tenzij het certificeringsactiviteiten betreft. Het Comité is van mening dat in het ontwerp van de accreditatie-eisen moet worden gespecificeerd wanneer “het certificeringsactiviteiten betreft” of moet worden verduidelijkt dat het certificeringsorgaan de verantwoordelijkheid blijft houden voor de besluitvorming, zelfs wanneer externe deskundigen worden ingeschakeld. Het Comité beveelt de Tsjechische toezichthouder daarom aan om het ontwerp dienovereenkomstig te wijzigen.

2.2.5 EISEN AAN DE PROCEDURE

25. Het Comité merkt op dat in deel 3.2.1.2.10.1.1 van het ontwerp van de aanvullende eisen van de Tsjechische toezichthouder wordt verwezen naar “alle aanvullende eisen in verband met belangenconflicten (7.1, punt 1)”. Het ontwerp van de aanvullende eisen van de Tsjechische toezichthouder bevat echter geen aanvullende eisen met betrekking tot belangenconflicten. Het Comité moedigt de Tsjechische toezichthouder daarom aan het ontwerp te wijzigen om verwarring te voorkomen.
26. Wat de eisen voor de aanvraag betreft, merkt het Comité op dat deel 3.2.1.2.10.2.3 van het ontwerp van de accreditatie-eisen van de Tsjechische toezichthouder lijkt te impliceren dat er in de aanvraag alleen informatie over de doorgegeven gegevens moet worden verstrekt, wanneer het doorgifte naar een derde land of een internationale organisatie betreft. Het Comité benadrukt echter dat de

aanvraag altijd een beschrijving moet bevatten van de gegevens die naar andere systemen of organisaties worden overgedragen, ongeacht hun locatie. Het Comité moedigt de Tsjechische toezichthouder daarom aan de tekst te wijzigen om verwarring te voorkomen.

27. Het Comité merkt op dat de verplichting om in de certificeringsovereenkomst bindende evaluatiemethoden vast te stellen (deel 3.2.1.2.1.2.6 van het ontwerp van de accreditatie-eisen van de Tsjechische toezichthouder) geen verwijzing bevat naar het Target of Evaluation (ToE), overeenkomstig punt 7.3, item 1, van de bijlage bij de richtsnoeren. Ten behoeve van de duidelijkheid moedigt het Comité de Tsjechische toezichthouder aan een dergelijke verwijzing op te nemen.
28. Voorts merkt het Comité op dat het ontwerp van de accreditatie-eisen van de Tsjechische toezichthouder voorzien in de situatie waarin verwerkers worden ingezet voor gegevensverwerkingshandelingen, in overeenstemming met de bijlage bij de richtsnoeren (deel 3.2.1.2.10.2 van de ontwerp-accreditatie-eisen van de Tsjechische toezichthouder). Het Comité spoort de Tsjechische toezichthouder aan om te overwegen in dit geval ook een verwijzing te maken naar gezamenlijke verwerkingsverantwoordelijken en hun specifieke regelingen.
29. Met betrekking tot de evaluatie-eisen (deel 3.2.1.2.10.4 van de ontwerp-eisen van de Tsjechische toezichthouder) merkt het Comité op dat de accreditatie-eisen van de Tsjechische toezichthouder geen verplichting bevatten voor het certificeringsorgaan om in zijn certificeringsmechanisme in detail te beschrijven hoe de aanvrager door middel van de onder punt 7.4.6 van ISO 17065 gevraagde informatie wordt ingelicht over onregelmatigheden waarvan een certificeringsmechanisme blijkt geeft. Zoals uiteengezet in de bijlage (punt 7.4) moeten ten minste de aard en de timing van dergelijke informatie worden gedefinieerd. Het Comité beveelt de Tsjechische toezichthouder aan om voornoemde verplichting toe te voegen.
30. Bovendien lijkt deel 3.2.1.2.10.4.2 van de ontwerp-eisen van de Tsjechische toezichthouder de evaluatiemethoden te beperken tot tests, audits of inspecties. Het Comité is van oordeel dat er ook andere evaluatiemethoden kunnen worden gebruikt en moedigt de Tsjechische toezichthouder daarom aan het ontwerp te wijzigen om te verduidelijken dat de opsomming niet uitputtend is.
31. Wat deel 3.2.1.2.10.4.4.1.4 van het ontwerp van de accreditatie-eisen van de Tsjechische toezichthouder betreft, is het Comité van mening dat daarin duidelijk moet worden vermeld dat het certificeringsorgaan moet nagaan of aan de criteria wordt voldaan. Het moedigt de Tsjechische toezichthouder aan het ontwerp dienovereenkomstig aan te passen.
32. Met betrekking tot de toetsingseisen (deel 3.2.1.2.10.5 van het ontwerp van de accreditatie-eisen van de Tsjechische toezichthouder) merkt het Comité op dat in het ontwerp van de accreditatie-eisen van de Tsjechische toezichthouder niet wordt verwezen naar de verplichting om procedures vast te stellen voor de verlening en intrekking van certificaten. Het Comité beveelt de Tsjechische toezichthouder aan om het ontwerp dienovereenkomstig te wijzigen.
33. Wat betreft de eisen voor documentatie inzake certificering merkt het Comité op dat in deel 3.1.2.10.7.2 van het ontwerp van de accreditatie-eisen van de Tsjechische toezichthouder wordt bepaald dat het certificeringsorgaan moet specificeren dat toezicht een voorwaarde is voor de geldigheid van certificaten, "indien monitoring door een certificeringsregeling vereist wordt [...]". Het Comité is van oordeel dat de monitoringactiviteiten bij certificering op grond van de AVG altijd verplicht zijn, en beveelt de Tsjechische toezichthouder daarom aan een dergelijke verplichting op te nemen.

34. Wat betreft de eisen in verband met de lijst van gecertificeerde producten (deel 3.2.1.2.10.8 van het ontwerp van de accreditatie-eisen van de Tsjechische toezichthouder en punt 7.8 van de bijlage), en met name de verplichting om de bevoegde toezichthoudende autoriteit in kennis te stellen van de redenen voor het verlenen of intrekken van de gevraagde certificering, merkt het Comité op dat het ontwerp van de accreditatie-eisen van de Tsjechische toezichthouder naar deel 3.2.1.2.10.4.5 verwijzen. Dat deel heeft echter betrekking op de verplichting om de evaluatiedocumentatie op verzoek toegankelijk te maken voor de Tsjechische toezichthouder, terwijl de eis in punt 7.8 van de bijlage bij de richtsnoeren een verplichting bevat om de toezichthoudende autoriteit proactief van de redenen voor het verlenen of intrekken van de certificering in kennis te stellen. Het Comité beveelt de Tsjechische toezichthouder daarom aan om het ontwerp dienovereenkomstig te wijzigen.
35. Wat betreft de wijzigingen die van invloed zijn op de certificering, merkt het Comité op dat in de ontwerp-accreditatie-eisen van de Tsjechische toezichthouder het goedkeuringsproces voor de bevoegde toezichthoudende autoriteit, waarnaar in de bijlage bij de richtsnoeren wordt verwezen (blz. 21), niet wordt genoemd als een van de overeen te komen procedures. Het Comité erkent dat de lijst in punt 7.10 van de bijlage niet verplicht is. Ten behoeve van de samenhang moedigt het Comité de Tsjechische toezichthouder evenwel aan om een verwijzing naar het goedkeuringsproces voor de bevoegde toezichthoudende autoriteit toe te voegen.
36. Het Comité merkt op dat het ontwerp van de accreditatie-eisen van de Tsjechische toezichthouder geen duidelijke verplichting bevat voor het certificeringsorgaan om besluiten en bevelen van de bevoegde toezichthoudende autoriteit om de certificering van een aanvrager in te trekken of niet af te geven, indien niet of niet meer aan de certificeringseis wordt voldaan, te aanvaarden. Het Comité beveelt de Tsjechische toezichthouder aan om deze verplichting duidelijk aan het ontwerp van de accreditatie-eisen toe te voegen. Met betrekking tot de beëindiging, vermindering, opschorting of intrekking van certificering merkt het Comité op dat in de delen 3.2.1.2.10.10.2 en 3.2.1.2.10.10.3 van de ontwerp-eisen sprake is van een "aansporing". Als het de bedoeling is te verwijzen naar "besluiten en bevelen" van de toezichthoudende autoriteit, overeenkomstig artikel 58, lid 2, onder h), van de AVG, moedigt het Comité de Tsjechische toezichthouder aan dezelfde termen te gebruiken als in de richtsnoeren en te verwijzen naar besluiten en bevelen".

2.2.6 BEHEERSYSTEEM

37. Het Comité is van oordeel dat deel 3.2.1.2.11 van het ontwerp van aanvullende eisen van de Tsjechische toezichthouder geen verplichting bevat voor het certificeringsorgaan om "te allen tijde openbaar te maken welke certificeringen zijn uitgevoerd en op basis waarvan, hoe lang de certificering geldig is, in welk kader en onder welke voorwaarden", zoals vermeld in punt 8 van de bijlage. Het Comité beveelt de Tsjechische toezichthouder daarom aan om de ontwerp-eisen te wijzigen door de bovengenoemde verwijzing erin op te nemen.

3 CONCLUSIES/AANBEVELINGEN

38. Het ontwerp van de accreditatie-eisen van de Tsjechische toezichthouder kan leiden tot een incoherente toepassing van de accreditatie van certificeringsorganen. De volgende wijzigingen moeten worden aangebracht:
39. Ten aanzien van de "algemene accreditatie-eisen" beveelt het Comité aan dat de Tsjechische toezichthouder:

- 1) in deel 3.2.1.2.1.2 de verplichting opneemt om de toezichhoudende autoriteit toegang te verlenen tot “contractueel vertrouwelijke aangelegenheden”;
 - 2) in deel 3.2.1.2.1.2.8 “informatie voor het afgeven van het certificaat” vervangt door “informatie die nodig is voor het afgeven van het certificaat”;
 - 3) deel 3.2.1.2.1.2.9 verduidelijkt overeenkomstig artikel 42, lid 8, van de AVG;
 - 4) in deel 3.2.1.2.1.2.12 een verwijzing toevoegt naar de bepaling dat [indien van toepassing] “ook rekening moet worden gehouden met alle gevolgen voor diens klanten”;
 - 5) deel 3.2.1.2.1.2.13 wijzigt met de toevoeging “alle veranderingen in zijn feitelijke of juridische situatie en met betrekking tot de producten, processen en diensten waarop de certificering betrekking heeft”;
 - 6) deel 3.2.1.2.1.3 en deel 3.2.1.2.1.2.14 schrapt;
 - 7) de ontbrekende eisen met betrekking tot het onpartijdigheidsmanagement aanpast aan de bijlage.
40. Ten aanzien van de “benodigde middelen” beveelt het Comité aan dat de Tsjechische toezichthouder:
- 1) deel 3.2.1.2.9.1 wijzigt om te specificeren wanneer “het certificeringsactiviteiten betreft” of om uitdrukkelijk te bepalen dat het certificeringsorgaan de verantwoordelijkheid blijft houden voor de besluitvorming, zelfs wanneer externe deskundigen worden ingeschakeld;
41. Ten aanzien van de “Procesvereisten” beveelt het Comité aan dat de Tsjechische toezichthouder:
- 1) in deel 3.2.1.2.10.4 de verplichting opneemt voor het certificeringsorgaan om in zijn certificeringsmechanisme in detail te beschrijven hoe de aanvrager door middel van de onder punt 7.4.6 van ISO 17065 gevraagde informatie wordt ingelicht over onregelmatigheden waarvan een certificeringsmechanisme blijkt geeft;
 - 2) deel 3.2.1.2.10.5 wijzigt om te verwijzen naar de verplichting om procedures vast te stellen voor de verlening en intrekking van certificaten;
 - 3) deel 3.1.2.10.7.2 wijzigt om aan te geven dat de monitoringactiviteiten bij certificering op grond van de AVG altijd verplicht zijn;
 - 4) deel 3.2.1.2.10.8 wijzigt om rekening te houden met de verplichting voor het certificeringsorgaan om de toezichhoudende autoriteit proactief in kennis te stellen van de redenen voor het verlenen of intrekken van de certificering;
 - 5) de verplichting opneemt om besluiten en opdrachten van de bevoegde toezichhoudende autoriteit te aanvaarden om de certificering in te trekken of niet af te geven aan een aanvrager indien niet langer wordt voldaan aan de certificeringseisen.
42. Ten aanzien van de “eisen met betrekking tot het managementsysteem” beveelt het Comité aan dat de Tsjechische toezichthouder:
- 1) de verplichting opneemt voor het certificeringsorgaan om “te allen tijde openbaar te maken welke certificeringen zijn uitgevoerd en op basis waarvan, hoe lang de certificering

geldig is, in welk kader en onder welke voorwaarden”, zoals vermeld in punt 8 van de bijlage.

4 SLOTOPMERKINGEN

43. Dit advies is gericht tot de Tsjechische toezichthouder en wordt bekendgemaakt op grond van artikel 64, lid 5, onder b), van de AVG.
44. Overeenkomstig artikel 64, leden 7 en 8, van de AVG deelt de Tsjechische 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.
45. De Tsjechische 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)