Advies 14/2026 over de Europrivacy-certificeringscriteria in verband met hun goedkeuring door het Comité als Europees gegevensbeschermingszegel krachtens artikel 42, lid 5, AVG

Vastgesteld op 15 April 2026

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

Inhoud

Het Europees Comité voor gegevensbescherming

Gezien artikel 63, artikel 64, lid 2, en artikel 42 van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (hierna "AVG" genoemd),

Gezien de Overeenkomst betreffende de Europese Economische Ruimte (hierna "EER" genoemd) en met name bijlage XI en Protocol 37 daarbij, 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,

Overwegende hetgeen volgt:

1. De lidstaten, de toezichthoudende autoriteiten, het Europees Comité voor gegevensbescherming (hierna "het Comité" genoemd) en de Europese Commissie bevorderen, met name op Unieniveau, de invoering van certificeringsmechanismen voor gegevensbescherming (hierna "certificeringsmechanismen" genoemd) en gegevensbeschermingszegels en -merktekens waarmee kan worden aangetoond dat verwerkingsverantwoordelijken en verwerkers bij verwerkingen in overeenstemming met de AVG handelen, en hierbij wordt ook rekening gehouden met de specifieke behoeften van micro-, kleine en middelgrote ondernemingen. Daarnaast kan het invoeren van certificeringsmechanismen de transparantie versterken en betrokkenen in staat stellen om het gegevensbeschermingsniveau van producten en diensten ter zake te beoordelen.

2. De certificeringscriteria maken integraal deel uit van een certificeringsmechanisme. Bijgevolg wordt in de AVG de goedkeuring vereist van de criteria voor een nationaal certificeringsmechanisme door de bevoegde toezichthoudende autoriteit (artikel 42, lid 5, en artikel 43, lid 2, punt b), AVG), of, in het geval van een Europees gegevensbeschermingszegel, door het Comité (artikel 42, lid 5, en artikel 70, lid 1, punt o), AVG).

3. Wanneer een toezichthoudende autoriteit voornemens is de goedkeuring van een Europees gegevensbeschermingszegel door het Comité voor te stellen overeenkomstig artikel 42, lid 5, AVG, moet de toezichthoudende autoriteit aangeven of de eigenaar van de regeling voornemens is het certificeringsmechanisme in alle lidstaten aan te bieden. In dit geval bestaat de voornaamste rol van het Comité erin de consistente toepassing van de AVG te waarborgen, via het in de artikelen 63, 64 en 65 AVG bedoelde coherentiemechanisme. In dit kader keurt het Comité overeenkomstig artikel 64, lid 2, AVG de certificeringscriteria goed.

4. Dit advies moet een consistente toepassing van de AVG waarborgen, onder meer door de toezichthoudende autoriteiten, de verwerkingsverantwoordelijken en verwerkers, in het licht van de kernelementen waarin certificeringsmechanismen moeten voorzien. Meer specifiek wordt de beoordeling door het Comité uitgevoerd op basis van de "Richtsnoeren 1/2018 voor certificering en het vaststellen van certificeringscriteria overeenkomstig de artikelen 42 en 43 van de verordening" (hierna de "richtsnoeren" genoemd) en het bijbehorende addendum met "Richtsnoeren voor de beoordeling van certificeringscriteria" (hierna het "addendum" genoemd), waarvoor de periode van openbare raadpleging op 26 mei 2021 is verstreken.

5. Derhalve erkent het Comité dat elk certificeringsmechanisme afzonderlijk moet worden behandeld en dat dit de beoordeling van andere certificeringsmechanismen onverlet laat.

[1] Alle verwijzingen naar "lidstaten" in dit document moeten worden gelezen als verwijzingen naar "lidstaten van de EER".

6. Met behulp van certificeringsmechanismen kunnen verwerkingsverantwoordelijken en verwerkers de naleving van de AVG aantonen. Daarom moeten de criteria ervan de in de AVG vastgestelde vereisten en beginselen inzake de bescherming van persoonsgegevens naar behoren weerspiegelen en bijdragen tot de consequente toepassing ervan.
7. Tegelijkertijd moet de eigenaar van de regeling ervoor zorgen dat het certificeringsmechanisme is afgestemd op en in overeenstemming is met de opgenomen of gebruikte ISO-normen en certificeringspraktijken.
8. Bijgevolg moeten certificeringen een meerwaarde bieden aan verwerkingsverantwoordelijken en verwerkers door te helpen bij de uitvoering van gestandaardiseerde en gespecificeerde organisatorische en technische maatregelen die de naleving van de AVG bij de verwerking aantoonbaar vergemakkelijken en verbeteren, rekening houdend met sectorspecifieke vereisten.
9. Het Comité verwelkomt de inspanningen die eigenaren van regelingen zich getroosten om certificeringsmechanismen op te stellen die praktische en potentieel kostenefficiënte instrumenten zijn om te zorgen voor betere coherentie met de AVG en om het recht op privacy en gegevensbescherming van betrokkenen te bevorderen door de transparantie te vergroten.
10. Het Comité herinnert eraan dat certificeringen vrijwillige verantwoordingsinstrumenten zijn, en dat de toetreding tot een certificeringsmechanisme de verantwoordelijkheid van verwerkingsverantwoordelijken of verwerkers voor de naleving van de AVG niet vermindert en de toezichthoudende autoriteiten niet belet hun taken en bevoegdheden uit te oefenen overeenkomstig de AVG en de desbetreffende nationale wetgeving.
11. In dit advies gaat het Comité in op kwesties als het toepassingsgebied van de criteria, de toepasselijkheid en de relevantie van de criteria in alle lidstaten.
12. Dit advies van het Comité is uitsluitend toegespitst op de certificeringscriteria. Het Comité kan informatie op hoog niveau over de evaluatiemethoden nodig hebben om de controleerbaarheid van de criteria in het kader van zijn advies daarover grondig te kunnen beoordelen. Dit houdt echter geen enkele goedkeuring van dergelijke evaluatiemethoden in.
13. Het advies van het Comité zal overeenkomstig artikel 64, lid 2, AVG in samenhang met artikel 10, lid 2, van het reglement van orde van het Comité worden vastgesteld binnen acht weken, te rekenen vanaf 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. Indien in het advies van het Comité wordt geconcludeerd dat de criteria niet kunnen worden goedgekeurd, kan de toezichthoudende autoriteit de criteria opnieuw ter goedkeuring voorleggen wanneer de in het oorspronkelijke advies van het Comité geuite bezwaren zijn weggenomen.

Brengt het volgende advies uit:

1 Samenvatting van de feiten

14. Overeenkomstig artikel 42, lid 5, AVG en de richtsnoeren zijn de Europrivacy-certificeringscriteria (versie 82) (hierna de “certificeringscriteria” genoemd) opgesteld door het European Centre for Certification and Privacy (hierna de ”eigenaar van de regeling” genoemd).

15. De Luxemburgse toezichthoudende autoriteit heeft de Europrivacy-certificeringscriteria (versie 82) op 29 januari 2026 ter goedkeuring voorgelegd aan het Comité overeenkomstig artikel 64, lid 2, AVG.

16. De beslissing over de volledigheid van het dossier is genomen op 31 maart 2026.

17. Het Comité herinnert eraan dat het de Europrivacy-certificeringscriteria (versie 60) op 10 oktober 2022, middels Advies 28/2022, heeft goedgekeurd als Europees gegevensbeschermingszegel overeenkomstig artikel 42, lid 5, AVG ("vorig advies van het Comité").

18. In dit advies wordt ingegaan op de gewijzigde versie van de Europrivacy-certificeringscriteria (versie 82). Om te beginnen merkt het Comité op dat in deze versie van de certificeringscriteria, die nu aan het Comité is voorgelegd, het toepassingsgebied is uitgebreid tot aanvragers die onder artikel 3, lid 2, AVG vallen, en dat in dit verband een criterium inzake mogelijke conflicten met het recht van derde landen is ingevoerd. Voorts merkt het Comité op dat sommige certificeringscriteria die in 2022 door het Comité zijn goedgekeurd, in de gewijzigde versie van de Europrivacy-certificeringscriteria (versie 82) zijn aangepast, verfijnd en/of verduidelijkt. Deze wijzigingen hebben met name betrekking op: de aanwijzing van een vertegenwoordiger in de EER en de samenwerking bij verzoeken van de bevoegde gegevensbeschermingsautoriteiten in de EER; het verslag van de nalevingsbeoordeling inzake nationale verplichtingen (National Obligations Compliance Assessment Report, "NOCAR"), de verdere verwerking, de waarborgen bij de verwerking van bijzondere categorieën van persoonsgegevens, de rechten van betrokkenen, de inschakeling van subverwerkers, de behandeling van inbreuken in verband met persoonsgegevens, de risicobeoordeling voor de gegevensverwerking en het beleid en de vereisten inzake beveiliging.

19. Het Comité benadrukt dat de wijziging van de reeds in 2022 goedgekeurde certificeringscriteria gevolgen zal hebben voor de tot dusver afgegeven certificeringen en voor de lopende certificeringsprocessen. Daarom moet worden gezorgd voor een op passende en transparante wijze beheerde overgangsperiode tussen de Europese gegevensbeschermingszegels die zijn afgegeven volgens de met het vorige advies van het Comité (versie 60) goedgekeurde certificeringscriteria en die welke worden afgegeven volgens de certificeringscriteria (versie 82) die in dit advies worden beoordeeld. In dit verband begrijpt het Comité, uit de door de eigenaar van de regeling verstrekte documentatie, dat alle lopende certificeringsprocessen uiterlijk eind 2026 moeten zijn afgerond en dat na dat tijdstip de certificeringscriteria die zijn goedgekeurd met het vorige advies van het Comité (versie 60), niet langer zullen worden gebruikt om nieuwe certificaten af te geven. De tot dusver afgegeven certificaten blijven geldig tot het einde van hun geldigheidsduur van drie jaar en zullen worden verlengd volgens de certificeringscriteria (versie 82). Bijgevolg zullen de certificeringscriteria die met het vorige advies van het Comité (versie 60) zijn goedgekeurd, na eind 2029 volledig zijn vervangen door de certificeringscriteria (versie 82). Daarnaast zal de informatie over deze overgangsperiode openbaar worden gemaakt door de eigenaar van de regeling. Er kunnen enkele aanpassingen nodig zijn in de accreditatie van de certificeringsorganen, maar deze kwestie komt in dit advies niet aan de orde, aangezien zij niet onder de bevoegdheid van het Comité valt.

20. De algemene Europrivacy-certificeringsregeling is niet bedoeld als instrument voor doorgiften overeenkomstig artikel 42, lid 2, en artikel 46, lid 2, punt f), AVG. Op 29 januari 2026 heeft de Luxemburgse toezichthoudende autoriteit op grond van artikel 64, lid 2, AVG aan het Comité ook een aanvullende reeks certificeringscriteria ter goedkeuring voorgelegd ("de uitbreiding van de Europrivacy-certificeringsregeling voor certificering van gegevensimporteurs op grond van artikel 46"), waarvan het toepassingsgebied betrekking heeft op

verwerkingsverantwoordelijken en verwerkers buiten de EER die niet rechtstreeks onder de AVG vallen overeenkomstig artikel 3, lid 2, AVG, maar persoonsgegevens verwerken die zijn ontvangen van een andere verwerkingsverantwoordelijke of verwerker die onder de AVG valt. Met betrekking tot deze reeks certificeringscriteria die bedoeld zijn om te worden gebruikt als instrument voor doorgiften overeenkomstig artikel 46, lid 2, punt f), AVG, heeft het Comité Advies 15/2026 vastgesteld.

2 Beoordeling

21. Het Comité heeft zijn beoordeling van de certificeringscriteria ten behoeve van de goedkeuring ervan krachtens artikel 42, lid 5, AVG uitgevoerd in overeenstemming met de structuur van bijlage 2 bij de richtsnoeren (hierna "bijlage" genoemd) en het addendum daarbij.

22. In het kader van dit advies en om de certificeringscriteria goed te keuren, heeft het Comité een beoordeling uitgevoerd van de voorafgaande verificaties en controles van de aanvraag en het ToE (Target of Evaluation) (A); de Europrivacy AVG-kerncriteria (G), en de controles en verificaties van de technologische en organisatorische maatregelen (T), die samen met de certificeringscriteria zijn verstrekt.

23. Voorts merkt het Comité in dit verband op dat de "aanvullende contextuele controles en verificaties"[2], die samen met de bij het vorige advies van de Comité goedgekeurde certificeringscriteria (versie 60) zijn verstrekt, en bedoeld zijn om ervoor te zorgen dat de gegevensverwerking in het kader van het ToE voldoet aan domeinspecifieke en technologiespecifieke vereisten[3], door het Comité in zijn vorige advies niet zijn goedgekeurd en dat dergelijke "aanvullende contextuele controles en verificaties" niet meer voorkomen in de bijgewerkte documentatie die in het kader van dit advies is verstrekt.

24. Het Comité merkt op dat, zoals wordt verduidelijkt in de definities van de regeling, bij verwijzingen naar "bevoegde gegevensbeschermingsautoriteiten" in de hele regeling de gegevensbeschermingsautoriteiten in de EER worden bedoeld[4].

25. Wat betreft de definities van het recht van derde landen begrijpt het Comité dat het verwijst naar het recht dat van toepassing is op de aanvrager en/of op de persoonsgegevens die in het kader van het ToE worden verwerkt, voor zover dat recht geen beperkingen oplegt aan de rechten inzake gegevensbescherming die verder gaan dan wat in een democratische samenleving noodzakelijk en evenredig is om een van de in artikel 23, lid 1, AVG genoemde doelstellingen te waarborgen, evenredig is aan het nagestreefde doel, de wezenlijke inhoud van het recht op gegevensbescherming eerbiedigt, en voorziet in specifieke maatregelen om de grondrechten en belangen van betrokkenen te beschermen.

[2] Het Comité heeft de "aanvullende contextuele controles en verificaties" in zijn vorige advies niet goedgekeurd.
[3] Vorig advies van het Comité, punten 7 en 8.
[4] Zie de definitie in de Europrivacy-criteria voor "bevoegde toezichthoudende autoriteit": "'Bevoegde gegevensbeschermingsautoriteit' verwijst naar gegevensbeschermingsautoriteiten in de EER. In het algemeen verwijst de term naar de nationale gegevensbeschermingsautoriteiten die bevoegd zijn om de naleving van de in het kader van het ToE verwerkte persoonsgegevens af te dwingen. In het geval van een AVG-certificering die op grond van artikel 46 AVG aan een gegevensimporteur wordt afgegeven, is de bevoegde gegevensbeschermingsautoriteit die van de gegevensexporteur in de EER, behalve voor het indienen van een klacht wanneer een autoriteit in de EER bevoegd is".

2.1 Toepassingsgebied van het certificeringsmechanisme en onderwerp van beoordeling (Target of Evaluation, ToE)

26. Het Comité herinnert eraan[5] dat de Europrivacy-certificeringsregeling een algemene regeling is in die zin dat zij gericht is op een groot aantal verschillende verwerkingen die worden uitgevoerd door verwerkingsverantwoordelijken en verwerkers uit diverse sectoren.

27. Het Comité is ermee ingenomen dat in de door de Luxemburgse toezichthoudende autoriteit verstrekte documentatie over het toepassingsgebied van deze certificeringsregeling de gewijzigde Europrivacy-regeling van toepassing is op: **i)** verwerkingsverantwoordelijken en verwerkers die gevestigd zijn in de Europese Unie (EU) of in de Europese Economische Ruimte (EER); **ii)** buiten de EER gevestigde verwerkingsverantwoordelijken en verwerkers die op grond van artikel 3, lid 2, AVG onder de AVG vallen, hetzij omdat zij goederen of diensten aanbieden aan betrokkenen in de EER, hetzij omdat zij het gedrag van betrokkenen in de EER monitoren[6]. De toepasselijkheid van de criteria wordt bepaald aan de hand van de rol en de verantwoordelijkheden van de aanvrager.

28. Met betrekking tot aanvragers als bedoeld in artikel 3, lid 2, AVG die zich in een derde land bevinden en ten aanzien waarvan geen adequaatheidsbesluit is genomen dat het ToE omvat, worden in criterium A.2.1.6 de voorwaarden vastgesteld waaraan moet worden voldaan bij het omschrijven van het ToE tijdens de beoordeling van hun aanvraag tot certificering. Alvorens een certificeringsaudit te overwegen, moet het certificeringsorgaan met name nagaan of de aanvrager kan aantonen dat de nationale wetgeving en praktijk van het derde land de naleving van de certificeringsvoorschriften door de aanvrager niet in de weg staan. Als dit niet het geval is, stopt het certificeringsproces tijdens de aanvraagfase.

29. Het Comité merkt op dat een verwerkingsverantwoordelijke een ToE aan het Europrivacy-certificeringsproces kan onderwerpen waarvoor meerdere verwerkingsverantwoordelijken gezamenlijk verantwoordelijk zijn (criterium A.2.1.5). Indien het ToE onder gezamenlijke verantwoordelijkheid valt, wenst het Comité te benadrukken dat het geaccrediteerde certificeringsorgaan het aanvraagproces zorgvuldig zal moeten uitvoeren om te waarborgen dat het ToE zinvol is en dat de aanvrager volledig verantwoordelijk is voor de naleving door het ToE van alle verplichtingen uit hoofde van de AVG die de certificeringsregeling beoogt aan te tonen. Bijgevolg zou de regeling die tussen de aanvrager en de andere bij het ToE betrokken gezamenlijke verwerkingsverantwoordelijken is getroffen met betrekking tot hun respectieve verantwoordelijkheden voor de naleving van de verplichtingen uit hoofde van de AVG, afhankelijk van de context van de verwerkingsactiviteiten van het ToE, de aanvrager kunnen beletten aan de certificeringscriteria te voldoen.

2.2 Verwerkingen

30. Zoals het Comité in zijn vorige advies heeft opgemerkt, hebben de certificeringscriteria betrekking op de relevante onderdelen van de verwerkingen (gegevens, systemen en verwerking) met betrekking tot het algemene toepassingsgebied van de certificeringsregeling. De certificeringscriteria maken het met name mogelijk bijzondere categorieën van gegevens te identificeren zoals omschreven in artikel 9 AVG (punt G.2 van de criteria inzake bijzondere gegevensverwerking).

[5] Vorig advies van het EDPB, punt 6.
[6] Zie de EDPB-richtsnoeren over het territoriale toepassingsgebied van de AVG (artikel 3), versie 2.1, vastgesteld op 12 november 2019, deel 2.

2.3 Rechtmatigheid van de verwerking

31. Zoals het Comité in zijn vorige advies over de reeds goedgekeurde certificeringscriteria (versie 60) heeft opgemerkt, vereisen de certificeringscriteria dat de rechtmatigheid van de gegevensverwerking voor elke afzonderlijke verwerking in het ToE wordt gecontroleerd en dat de vereisten van een rechtsgrondslag als bedoeld in artikel 6 AVG worden gecontroleerd (punt G.1 van de criteria inzake de rechtmatigheid van de gegevensverwerking). Het Comité is er met name mee ingenomen dat de geactualiseerde certificeringscriteria vereisen dat de toestemming van de betrokkenen betrekking heeft op elk doel waarvoor de verwerking wordt uitgevoerd en dat de intrekking van de toestemming de betrokkene niet mag schaden.

32. Bovendien vereisen de certificeringscriteria, zoals opgemerkt in het vorige advies van het Comité, dat de specifieke vereisten worden gecontroleerd van de voorwaarden waaronder de verwerking van bijzondere categorieën van persoonsgegevens overeenkomstig artikel 9, lid 2, AVG is toegestaan (punt G.2.1 van de criteria inzake bijzondere gegevensverwerking), en dat aanvullende beperkingen en waarborgen voor de rechten en vrijheden van de betrokkene worden geboden. De certificeringscriteria vereisen ook dat de vereisten van de in artikel 10 AVG gedefinieerde voorwaarden voor de verwerking van persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten (punt G.2.2 van de criteria) worden gecontroleerd, indien van toepassing. In dit verband is het Comité ook ingenomen met het feit dat de geactualiseerde certificeringscriteria (criterium G.2.1.3 inzake aanvullende waarborgen voor de verwerking van bijzondere categorieën van persoonsgegevens) ook vereisen dat de aanvrager over aanvullende beperkingen en waarborgen beschikt, aangepast aan de specifieke aard van de gegevens en de bijbehorende risico's, wanneer bijzondere categorieën van persoonsgegevens bij de verwerking betrokken zijn.

33. Met betrekking tot aanvragers als bedoeld in artikel 3, lid 2, AVG die gevestigd zijn in een derde land en ten aanzien waarvan geen adequaatheidsbesluit is genomen dat het ToE omvat, vereisen de geactualiseerde certificeringscriteria bovendien dat de aanvrager een verslag van een juridisch deskundige overlegt waarin deze vaststelt dat het nationale recht en de nationale praktijk van het derde land de naleving van zijn verplichtingen inzake gegevensbescherming uit hoofde van de AVG niet in de weg staan. Evenzo wordt hierin vastgesteld dat het nationale recht van het derde land geen beperkingen oplegt aan de rechten inzake gegevensbescherming die verder gaan dan wat in een democratische samenleving noodzakelijk en evenredig is om een van de in artikel 23, lid 1, AVG genoemde doelstellingen te waarborgen, evenredig is aan het nagestreefde doel, de wezenlijke inhoud van het recht op gegevensbescherming eerbiedigt, en voorziet in specifieke maatregelen om de grondrechten en belangen van betrokkenen te beschermen. Dit verslag moet ook worden herzien telkens wanneer wijzigingen in de regelgeving of de organisatie de naleving van de criteria kunnen belemmeren of gevolgen kunnen hebben voor het ToE of de rechten van betrokkenen, en het certificeringsorgaan moet hiervan in kennis worden gesteld (criterium G.1.1.5).

34. In dit verband wordt in de richtsnoeren bij de geactualiseerde certificeringscriteria verduidelijkt dat "wanneer een buiten de EER gevestigde aanvrager in aanmerking komt voor een adequaatheidsbesluit dat relevant is voor de in het ToE uitgevoerde verwerking, de naleving van dit vereiste kan worden aangetoond door middel van een vereenvoudigd verslag". Volgens die criteria had in een dergelijk verslag beoordeeld moeten worden of het adequaatheidsbesluit van kracht is en hadden de redenen moeten worden gedocumenteerd waarom het ToE onder het toepassingsgebied van het adequaatheidsbesluit valt (criterium G.1.1.5, letter F).

2.4 Beginselen van gegevensverwerking

35. Het Comité herinnert eraan dat de certificeringscriteria op passende wijze voldoen aan de beginselen inzake gegevensbescherming overeenkomstig artikel 5 AVG. Met name wordt in de geactualiseerde certificeringscriteria het beginsel van doelbinding uitgebreid en verder uitgewerkt door een specifiek criterium op te nemen op grond waarvan moet worden aangetoond dat de persoonsgegevens niet verder worden verwerkt op een wijze die onverenigbaar is met die doeleinden, dat bij verdere verwerking altijd afzonderlijk moet worden beoordeeld of deze rechtmatig is, en dat een beoordeling van de verenigbaarheid met het doel wordt uitgevoerd en naar behoren wordt gedocumenteerd voor verdere verwerking van de gegevens (criterium G.1.1.6).

2.5 Algemene verplichtingen van verwerkingsverantwoordelijken en verwerkers

36. Het Comité herinnert eraan dat de certificeringscriteria [7] de verplichtingen van de verwerkingsverantwoordelijke uit hoofde van artikel 24 AVG weerspiegelen (punt G.4 inzake de verantwoordelijkheid van de verwerkingsverantwoordelijke) en de evaluatie vereisen van de contractuele overeenkomsten tussen verwerker en verwerkingsverantwoordelijke overeenkomstig artikel 28 AVG (punt G.5 van de criteria inzake gegevensverwerkers of subverwerkers).

37. Voorts is het Comité ingenomen met de toevoeging dat de certificeringscriteria vereisen dat een aanvrager als bedoeld in artikel 3, lid 2, AVG, een kantoor of een vertegenwoordiger in de EER aanwijst overeenkomstig artikel 27 AVG, waarvan de contactgegevens beschikbaar zijn op de website van de aanvrager (criterium G.4.1.4). Het Comité neemt nota van deze certificeringscriteria en herinnert eraan dat dit niet altijd een dwingende verplichting is voor verwerkingsverantwoordelijken en verwerkers op grond van de AVG, zodat rekening moet worden gehouden met de voorwaarden van artikel 27 AVG.

38. Daarnaast merkt het Comité op, zoals vermeld in zijn vorige advies, dat de certificeringscriteria vereisen dat alle aanvragers een functionaris voor gegevensbescherming (DPO) aanwijzen, ook als de aanvrager volgens artikel 37 van de AVG niet verplicht is een DPO aan te wijzen. In de criteria wordt nagegaan of de DPO voldoet aan de vereisten van de artikelen 37 tot en met 39 (punt G.9 van de criteria inzake de functionaris voor gegevensbescherming).

39. Evenzo vereisen de certificeringscriteria dat de inhoud van de registers van verwerkingsactiviteiten wordt gecontroleerd overeenkomstig artikel 30 AVG (punt G.5.3 van de criteria inzake registers van verwerkingsactiviteiten). In dit verband is het Comité ermee ingenomen dat aanvragers die onder artikel 3, lid 2, AVG vallen, op grond van de geactualiseerde certificeringscriteria moeten meewerken aan verzoeken van de bevoegde gegevensbeschermingsautoriteiten in de EER en hun op verzoek het register van verwerkingsactiviteiten ter beschikking moeten stellen (criterium G.5.3.5).

40. In dezelfde geest merkt het Comité op dat er enkele aanvullende certificeringscriteria zijn opgenomen met betrekking tot de inschakeling van subverwerkers voor aanvragers die optreden als verwerkingsverantwoordelijken of als verwerkers (punt G.5.1.2 inzake de

[7] Vorig advies van het Comité, punt 15.

inschakeling van subverwerkers). Dit onderscheid maakt het mogelijk de scheiding van rollen en verantwoordelijkheden tussen de actoren in de verwerkingsketen beter weer te geven.

2.6 Rechten van de betrokkenen

41. Net als in zijn vorige advies wijst het Comité erop dat het recht van de betrokkene op informatie overeenkomstig hoofdstuk III van de AVG afdoende aan bod komt in de certificeringscriteria en dat de criteria de invoering van passende maatregelen vereisen[8]. De certificeringscriteria vereisen ook maatregelen die voorzien in de mogelijkheid om in te grijpen in de verwerking teneinde de rechten van de betrokkenen te waarborgen en correcties, wissing of beperkingen mogelijk te maken (punt G.3 van de criteria inzake de rechten van de betrokkenen).

42. Daarnaast is het Comité ingenomen met de verbeteringen die zijn aangebracht in de certificeringscriteria met betrekking tot de informatie die aan betrokkenen moet worden verstrekt (punt G.3.2 inzake informatie die moet worden verstrekt wanneer persoonsgegevens bij de betrokkene worden verzameld en punt G.3.3 inzake informatie die moet worden verstrekt wanneer persoonsgegevens niet van de betrokkene zijn verkregen), de modaliteiten voor communicatie met betrokkenen [9] en voor de uitoefening van de rechten van betrokkenen[10] (punt G.3.1 inzake transparante informatie, communicatie en modaliteiten voor de uitoefening van de rechten van de betrokkenen), evenals het recht van inzage (punt G.3.4 inzake het recht van inzage van de betrokkene), het recht op wissing (punt G.3.6 inzake het recht op wissing (“recht op vergetelheid”)), het recht op beperking van de verwerking (criterium G.3.7.1 inzake het recht op beperking van de verwerking), de kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens of verwerkingsbeperking (criterium G.3.8.2 inzake de plicht om betrokkenen op verzoek te informeren over ontvangers), het recht van bezwaar (punt G.3.10 inzake het recht om bezwaar te maken) en het recht om niet te worden onderworpen aan geautomatiseerde individuele besluitvorming, waaronder profilering (punt G.3.11 inzake het recht om niet te worden onderworpen aan geautomatiseerde individuele besluitvorming, waaronder profilering).

2.7 Risico’s voor de rechten en de vrijheid

43. Het Comité heeft in zijn vorige advies reeds verklaard dat op grond van de certificeringscriteria het risico voor de rechten en vrijheden van natuurlijke personen als gevolg van de gegevensverwerking in het kader van het ToE moet worden beoordeeld overeenkomstig artikel 35 AVG (punt G.8 van de criteria inzake de plicht om te beoordelen of een gegevensbeschermingseffectbeoordeling vereist is)[11].

44. Het Comité is ingenomen met de wijzigingen in de certificeringscriteria dat “de aanvrager met een herhaalbare methode de risico’s van de verwerking moet hebben beoordeeld die van invloed kunnen zijn op de rechten en vrijheden van natuurlijke personen” (punt G.6.2.4 inzake de risicobeoordeling voor gegevensverwerking).

[8] Vorig advies van het Comité, punt 19.
[9] Zo wordt in criterium G.3.1.1 inzake de verplichting om in duidelijke taal informatie te verstrekken, nader ingegaan op de informatie over de gegevensverwerking die de aanvrager aan de betrokkene verstrekt. Zo moet nu onder meer i) de informatie schriftelijk of op andere wijze worden verstrekt, ii) de informatie beschikbaar zijn in de officiële taal of talen van de aanvrager en iii) beschikbaar zijn in de taal van de beoogde betrokkenen.
[10] Zo vereist criterium G.3.1.3 inzake het waarborgen van een goed beheer en registratie van de rechten van betrokkenen nu dat de aanvrager beschikt over een procedure of een mechanisme om ook de ontvangst van het verzoek aan de betrokkene te bevestigen en om ook de verzoeken van de betrokkene met de datum van ontvangst te registreren.
[11] Vorig advies van het Comité, punt 20.

45. Voorts is het Comité ingenomen met de verdere toevoegingen en nadere details in de certificeringscriteria. Het Comité neemt bijvoorbeeld nota van de toevoeging aan het PEB-proces wat betreft situaties waarin de aanvrager niet verplicht is een gegevensbeschermingseffectbeoordeling uit te voeren (punt G.8.2.1 inzake de vereisten van het PEB-proces).

2.8 Technische en organisatorische maatregelen ter waarborging van de bescherming

46. Zoals opgemerkt in het vorige advies van het Comité, vereisen de certificeringscriteria de toepassing van technische en organisatorische maatregelen die de vertrouwelijkheid, integriteit en beschikbaarheid van de verwerkingen waarborgen. De criteria vereisen ook de toepassing van technische maatregelen om gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen toe te passen overeenkomstig de artikelen 25 en 32 AVG (punt G.6 van de criteria inzake gegevensbescherming door ontwerp en door standaardinstellingen en beveiliging van de verwerking, punt G.6.2 van de criteria inzake beveiliging van de verwerking en deel T van de criteria)[12]. In dit verband is het Comité ermee ingenomen dat in de gewijzigde certificeringscriteria de regels en procedures die de aanvrager moet toepassen om aan deze criteria te voldoen, verder zijn uitgewerkt (punt G.6.1.2 inzake gegevensminimalisatie door standaardinstellingen).

47. Zoals benadrukt in het vorige advies van het Comité, vereisen de criteria de toepassing van maatregelen om ervoor te zorgen dat de kennisgevingsplicht voor inbreuken in verband met persoonsgegevens tijdig en in voldoende mate wordt uitgevoerd overeenkomstig de artikelen 33 en 34 AVG (punt G.7 van de criteria inzake het beheer van inbreuken in verband met persoonsgegevens).

48. In dit verband merkt het Comité op dat de certificeringscriteria verder zijn verbeterd en uitgewerkt. Meer in het bijzonder omvatten de certificeringscriteria nu een meer gedetailleerde lijst (punt G.7.1.1. inzake de verplichting om inbreuken in verband met gegevens te documenteren) met betrekking tot de informatie die de aanvrager moet documenteren wanneer zich een inbreuk in verband met gegevens voordoet (bv. de categorieën van persoonsgegevens die worden of kunnen worden beïnvloed, het geschatte aantal betrokkenen dat wordt of kan worden getroffen; de categorieën en het geschatte aantal persoonsgegevensregisters waarop de inbreuk betrekking heeft of kan hebben, de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens).

2.9 Criteria voor het aantonen van het bestaan van passende waarborgen voor de doorgifte van persoonsgegevens

49. Zoals het Comité in zijn vorige advies heeft bevestigd, moeten volgens de certificeringscriteria alle doorgiften van persoonsgegevens aan derde landen en internationale organisaties die bij het ToE betrokken zijn, worden geïdentificeerd en moet de gemaakte keuze met betrekking tot het mechanisme voor gegevensdoorgifte met passende waarborgen worden gemotiveerd,

[12] Vorig advies van het Comité, punt 21.

overeenkomstig hoofdstuk V van de AVG (punt G.10 van de criteria inzake doorgiften van persoonsgegevens aan derde landen of internationale organisaties).

50. Het Comité erkent dat deze certificeringscriteria voor aanvragers als bedoeld in artikel 3, lid 2, AVG van toepassing zullen zijn op zowel doorgiften van persoonsgegevens die betrokken zijn bij het ToE aan entiteiten die in hetzelfde derde land als de aanvrager gevestigd zijn, als in een ander derde land.

51. Daarnaast is het Comité ermee ingenomen dat de certificeringscriteria met betrekking tot de doorgifte van persoonsgegevens nu verder zijn uitgewerkt en duidelijker de verplichtingen van de aanvrager met betrekking tot deze kwestie bevatten (punt G.10.1 inzake algemene verplichtingen voor internationale doorgiften van persoonsgegevens aan derde landen of internationale organisaties).

3 Aanvullende criteria voor een Europees gegevensbeschermingszegel

52. Volgens de richtsnoeren moet bij de beoordeling worden nagegaan of “de criteria rekening kunnen houden met het gegevensbeschermingsrecht of de gegevensbeschermingsscenario’s van de lidstaten”. Zoals bevestigd in het vorige advies van het Comité, moet de aanvrager overeenkomstig punt G.1.1.3 van de certificeringscriteria een dergelijke beoordeling verstrekken in een NOCAR. Dit verslag moet een beoordeling bevatten van de nationale verplichtingen die van toepassing zijn op het ToE, en de maatregelen documenteren die de aanvrager heeft genomen om te voldoen aan de toepasselijke regels en, eventueel, de lopende corrigerende maatregelen. De aanvrager mag de door de eigenaar van de regeling voor elk land verstrekte lijst van essentiële aanvullende nationale eisen niet gebruiken als een uitputtende lijst van nationale verplichtingen die relevant zijn voor het ToE. Het vereiste betreffende de door de eigenaar van de regeling verstrekte indicatieve lijst van minimale aanvullende controles en verificaties zijn geen certificeringscriteria in het kader van dit advies.

53. Het Comité is ingenomen met de aanpassingen aan het NOCAR in de geactualiseerde criteria (punt G.1.1.3 inzake de beoordeling van de naleving van de nationale verplichtingen). Met name is nu verduidelijkt dat de aanvrager de beoordeling of bij de gegevensverwerking “de aanvullende nationale verplichtingen van de EER met betrekking tot de bescherming van persoonsgegevens die op de aanvrager van toepassing zijn”, zijn nageleefd, in een NOCAR moet documenteren. Dit verslag moet met name onder meer een duidelijke identificatie bevatten van het beoordeelde ToE, de lijst van geïdentificeerde aanvullende nationale verplichtingen inzake gegevensbescherming van de EER die van toepassing zijn op het ToE en de evaluatie van de naleving door het ToE van de geïdentificeerde aanvullende nationale verplichtingen inzake gegevensbescherming van de EER. Het Comité is van oordeel dat, indien de aanvrager buiten de EER is gevestigd en onderworpen is aan artikel 3, lid 2, AVG, de nationale verplichtingen inzake gegevensbescherming van de EER die van toepassing zijn op het ToE moeten worden bepaald op basis van de locatie van de betrokkenen aan wie de aanvrager goederen of diensten aanbiedt of van wie het gedrag wordt gemonitord.

4 Conclusies/aanbevelingen

54. Concluderend is het Comité van oordeel dat de Europrivacy-certificeringscriteria in overeenstemming zijn met de AVG en keurt het deze goed overeenkomstig de in artikel 70,

lid 1, punt o), AVG omschreven taak van het Comité, hetgeen resulteert in een gemeenschappelijke certificering (Europees gegevensbeschermingszegel).

55. Het Comité is van mening dat de certificeringscriteria integraal deel uitmaken van de certificeringsregeling en zal de Europrivacy-certificeringsregeling registreren in het openbaar register van certificeringsmechanismen en gegevensbeschermingszegels en -merktekens en de criteria openbaar maken overeenkomstig artikel 42, lid 8, AVG.

5 Slotopmerkingen

56. Dit advies is gericht tot de Luxemburgse toezichthoudende autoriteit en wordt bekendgemaakt overeenkomstig artikel 64, lid 5, punt b), AVG.

Voor het Europees Comité voor gegevensbescherming

De voorzitter

Anu Talus