Advies van de EDPB (artikel 64)

Advies 28/2022 over de Europrivacy-certificeringscriteria in verband met hun goedkeuring door het Comité als Europees gegevensbeschermingszegel krachtens artikel 42, lid 5 (AVG)

Vastgesteld op 10 oktober 2022

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

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 "de AVG" genoemd),

Gezien de Overeenkomst betreffende de Europese Economische Ruimte (hierna "de 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,

(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 kleine, middelgrote en micro-ondernemingen.[2] Daarnaast kan de vaststelling van certificeringsmechanismen de transparantie versterken en betrokkenen in staat stellen om het niveau van gegevensbescherming van de betreffende producten en diensten te beoordelen.[3]

(2) De certificeringscriteria maken integraal onderdeel 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), van de AVG), of, in het geval van een Europees gegevensbeschermingszegel, door het Comité (artikel 42, lid 5, en artikel 70, lid 1, punt o), van de 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, van de 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 van de AVG bedoelde coherentiemechanisme. In dit kader keurt het Comité overeenkomstig artikel 64, lid 2, van de 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, die certificeringsmechanismen moeten ontwikkelen. Meer specifiek wordt de beoordeling door het Comité uitgevoerd op basis van de "Richtsnoeren 1/2018 betreffende certificering en het identificeren van certificeringscriteria in overeenstemming met artikel 42 en 43 van de verordening" (hierna "de richtsnoeren" genoemd) en het bijbehorende addendum met

[1] Alle verwijzingen in dit advies naar "lidstaten" moeten worden gelezen als verwijzingen naar "EER-lidstaten".
[2] Artikel 42, lid 1, van de AVG.
[3] Overweging 100 van de AVG.

"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.

(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 is toegespitst op de certificeringscriteria. Indien het Comité informatie op hoog niveau over de evaluatiemethoden nodig heeft om de controleerbaarheid van de criteria in het kader van zijn advies daarover grondig te kunnen beoordelen, houdt dit geen enkele goedkeuring van dergelijke evaluatiemethoden in.

(13) Het advies van het Comité zal overeenkomstig artikel 64, lid 2, van de 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:

SAMENVATTING VAN DE FEITEN

1. Overeenkomstig artikel 42, lid 5, van de AVG en de richtsnoeren zijn de Europrivacy v.60-criteria (hierna de "ontwerp-certificeringscriteria", "certificeringscriteria" of "criteria" genoemd) opgesteld door het European Center for Certification and Privacy (hierna "de eigenaar van de regeling" genoemd).

2. De toezichthoudende autoriteit van Luxemburg heeft de Europrivacy-certificeringscriteria op 28 september 2022 ter goedkeuring voorgelegd aan het Comité overeenkomstig artikel 64, lid 2, AVG. De beslissing over de volledigheid van het dossier is genomen op 28 september 2022.

3. Het Europrivacy-certificeringsmechanisme is geen certificering in de zin van artikel 46, lid 2, punt f), dat bedoeld is voor internationale doorgiften van persoonsgegevens en biedt derhalve geen passende waarborgen in het kader van doorgiften van persoonsgegevens aan derde landen of internationale organisaties onder de in artikel 46, lid 2, punt f), bedoelde voorwaarden. Doorgifte van persoonsgegevens naar een derde land of een internationale organisatie vindt immers alleen plaats als de bepalingen van hoofdstuk V van de AVG worden nageleefd.

2 BEOORDELING

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

5. Het Comité merkt op dat de door de eigenaar van de regeling verstrekte uitvoeringsrichtsnoeren en voorgestelde middelen voor de verificatie van het certificeringsmechanisme niet altijd consistent zijn in de catalogus van criteria. In punt T.2.3.2 wordt bijvoorbeeld vereist dat er regels, beleidslijnen, procedures of mechanismen bestaan om inbreuken op te sporen en te melden (bijvoorbeeld een systeem voor de detectie van inbreuken dat het netwerkverkeer controleert op verdachte activiteiten en waarschuwt wanneer een dergelijke activiteit wordt ontdekt), terwijl de voorgestelde verificatiemiddelen betrekking hebben op de inspectie- en binnendringingstests (vereist in punt T.2.3.1). Hoewel dergelijke inconsistenties niet onder het toepassingsgebied van zijn beoordeling vallen, benadrukt het Comité dat zij een belemmering kunnen vormen voor de accreditatie van het certificeringsorgaan, tenzij zij door de eigenaar van de regeling worden verholpen.

2.1 Toepassingsgebied van het certificeringsmechanisme en onderwerp van de beoordeling

6. Het Europrivacy-certificeringsmechanisme is een algemene regeling in die zin dat het gericht is op een groot aantal verschillende verwerkingen die worden uitgevoerd door verwerkingsverantwoordelijken en verwerkers uit diverse sectoren. De belangrijkste criteria van dit certificeringsmechanisme bestaan uit de "kerncriteria" en uit de "TOM-controles en verificaties" die betrekking hebben op de technologische en organisatorische maatregelen (TOM) ter beveiliging van de verwerkte persoonsgegevens. Een reeks van de criteria voor "TOM-controles en verificaties" is alleen van toepassing indien het onderwerp van de beoordeling (ofwel "Target of Evaluation", hierna "ToE"

genoemd) bijzondere categorieën gegevens, gegevens in verband met strafbare feiten of persoonsgegevens van een minderjarige verwerkt.

7. Daarnaast omvatten de criteria ook "aanvullende contextuele controles" die ervoor moeten zorgen dat de gegevensverwerking in het kader van het ToE voldoet aan domeinspecifieke en technologiespecifieke vereisten. In een door de eigenaar van de regeling verstrekte informatieve matrix wordt beschreven op welke categorieën gegevensverwerkingsactiviteiten elke reeks criteria voor "aanvullende contextuele controles en verificaties" van toepassing is.

8. Het Comité verwelkomt algemene regelingen die specifieke criteria bevatten om ze schaalbaar, en zo toepasbaar, te maken voor specifieke verwerkingsactiviteiten of sectoren. Het Comité wenst echter ook te verduidelijken dat in het kader van een algemene regeling de volledigheid van de criteria die verband houden met de specifieke verwerkingen niet vereist is en derhalve in het kader van dit advies niet is beoordeeld. Bovendien herinnert het Comité eraan dat wanneer het documenten in verband met specifieke verwerkingsactiviteiten publiceert, de eigenaar van de regeling en de geaccrediteerde certificeringsinstanties rekening moeten houden met deze documenten.

9. De criteria die van toepassing zijn op de specificatie van het ToE zijn gedefinieerd in de vereisten in A.2.1.1. De specifieke regels voor het proces dat door de aanvrager en het certificeringsorgaan moeten worden gevolgd om het ToE te bepalen, zijn opgenomen in de Europrivacy-regeling (10.2 – Pre-certificeringsactiviteiten).

10. Het Comité leest in de door Luxemburgse toezichthoudende autoriteit verstrekte documentatie over het toepassingsgebied van het certificeringsmechanisme dat de Europrivacy-regeling van toepassing is op verwerkingsverantwoordelijken en verwerkers die gevestigd zijn in de Europese Unie (EU) of in de Europese Economische Ruimte (EER). De toepasselijkheid van de criteria wordt bepaald aan de hand van de rol en de verantwoordelijkheden van de aanvrager.

11. Het Comité merkt op dat een verwerkingsverantwoordelijke bij het Europrivacy-certificeringsproces een ToE kan indienen waarvoor verwerkingsverantwoordelijken gezamenlijk verantwoordelijk zijn (criterium A.2.7.1). 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 het certificatiemechanisme 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[4], afhankelijk van de context van de verwerkingsactiviteiten van het ToE, de aanvrager kunnen beletten aan de certificeringscriteria te voldoen.

[4] "Bij de vaststelling van hun respectieve verantwoordelijkheden moet met name rekening worden gehouden met de uitoefening van de rechten van de betrokkenen en de verplichtingen om informatie te verstrekken. Daarnaast dient de verdeling van de verantwoordelijkheden betrekking te hebben op andere verplichtingen voor de verwerkingsverantwoordelijke, zoals die met betrekking tot de algemene beginselen inzake gegevensbescherming, de rechtsgrondslag, de beveiligingsmaatregelen, de verplichting tot melding van inbreuken in verband met persoonsgegevens, de gegevensbeschermingseffectbeoordelingen, het doen van een beroep op verwerkers, de doorgiften aan derde landen en de contacten met betrokkenen en toezichthoudende autoriteiten." (Richtsnoeren 07/2020 over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG).

12. Het Comité merkt op dat de verwerking van genetische gegevens is uitgesloten van de werkingssfeer van het Europrivacy-certificeringsmechanisme. Bijgevolg heeft de beoordeling van de criteria door het Comité geen betrekking op de geschiktheid van de criteria voor het ToE die een dergelijke gegevensverwerking zouden omvatten.

2.2 Verwerkingen

13. De criteria hebben betrekking op de relevante onderdelen van de verwerkingen (gegevens, systemen en verwerking) met betrekking tot het algemene toepassingsgebied van het certificeringsmechanisme. De criteria maken het met name mogelijk bijzondere categorieën van gegevens te identificeren zoals omschreven in artikel 9 van de AVG (punt G.2 van de criteria – Bijzondere gegevensverwerking).

2.3 Rechtmatigheid van de verwerking

14. De criteria vereisen 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 van de AVG worden gecontroleerd (punt G.1 van de criteria – Rechtmatigheid van de gegevensverwerking).

2.4 Beginselen van gegevensverwerking

15. De criteria beantwoorden op passende wijze aan de beginselen inzake gegevensbescherming overeenkomstig artikel 5 van de AVG. Volgens de criteria moet de aanvrager met name aantonen dat de persoonsgegevens adequaat en relevant zijn en beperkt blijven tot hetgeen noodzakelijk is in verband met de doeleinden waarvoor zij worden verwerkt (gegevensminimalisering).

2.5 Algemene verplichtingen van verwerkingsverantwoordelijken en verwerkers

16. De criteria weerspiegelen de verplichtingen van de verwerkingsverantwoordelijke uit hoofde van artikel 24 van de AVG (G.4 – Verantwoordelijkheid van de verwerkingsverantwoordelijke) en vereisen de evaluatie van de overeenkomsten tussen de verwerker en de verwerkingsverantwoordelijke overeenkomstig artikel 28 van de AVG (punt G.5 van de criteria – Gegevensverwerkers of subverwerkers).

17. Op grond van de criteria moeten 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 – Functionaris voor gegevensbescherming).

18. De criteria controleren de inhoud van de registers van verwerkingsactiviteiten overeenkomstig artikel 30 van de AVG (punt G.5.3 van de criteria – Registers van verwerkingsactiviteiten).

2.6 Rechten van de betrokkenen

19. In de criteria komt het recht van de betrokkene op informatie overeenkomstig hoofdstuk III van de AVG afdoende aan bod en de criteria vereisen de invoering van passende maatregelen. De criteria 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 – Rechten van de betrokkenen).

2.7 Risico's voor de rechten en de vrijheid

20. Op grond van de criteria moet het risico voor de rechten en vrijheden van natuurlijke personen als gevolg van de gegevensverwerking in het kader van het ToE worden beoordeeld overeenkomstig artikel 35 van de AVG (punt G.8 van de criteria – Gegevensbeschermingseffectbeoordeling).

2.8 Technische en organisatorische maatregelen ter waarborging van de bescherming

21. De criteria vereisen 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 van de AVG (punt G.6 van de criteria – Beveiliging van de verwerking en gegevensbescherming door ontwerp; punt T.1/T.2 van de criteria – Kernvereisten inzake beveiliging/uitgebreide vereisten inzake beveiliging).

22. De criteria vereisen 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 van de AVG (punt G.7 van de criteria – Beheer van inbreuken in verband met gegevens).

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

23. Volgens de criteria moeten alle doorgiften van persoonsgegevens naar derde landen en naar 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, overeenkomstig hoofdstuk V van de AVG (punt G.10 van de criteria – Doorgifte van persoonsgegevens naar derde landen of internationale organisaties).

3. AANVULLENDE CRITERIA VOOR EEN EUROPEES GEGEVENSBESCHERMINGSZEGEL

24. Volgens de richtsnoeren moet bij de beoordeling worden nagegaan of "er in de criteria rekening [kan] worden gehouden met gegevensbeschermingsrecht of -scenario's van de lidstaten". Overeenkomstig punt G.1.1.3 van de criteria moet de aanvrager een dergelijke beoordeling verstrekken in een verslag van de effectbeoordeling inzake nationale verplichtingen (National Obligations Compliance Assessment Report, NOCAR). Het Comité merkt op dat dit verslag een beoordeling moet bevatten van de nationale verplichtingen die van toepassing zijn op het ToE en de maatregelen documenteert 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 inzake 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.

CONCLUSIES/AANBEVELINGEN

25. Concluderend is het Comité van oordeel dat de Europrivacy-certificeringscriteria in overeenstemming zijn met de AVG en keurt deze goed overeenkomstig de in artikel 70, lid 1, punt o), van de AVG omschreven taak van het Comité, hetgeen resulteert in een gemeenschappelijke certificering (Europees gegevensbeschermingszegel).

26. Het Comité zal het Europrivacy-certificeringsmechanisme registreren in het openbaar register van certificeringsmechanismen en gegevensbeschermingszegels en -merktekens overeenkomstig artikel 42, lid 8.

SLOTOPMERKINGEN

27. Dit advies is gericht tot de Luxemburgse toezichthoudende autoriteit en wordt bekendgemaakt op grond van artikel 64, lid 5, punt b), van de AVG.

Voor het Europees Comité voor gegevensbescherming

De voorzitter