Advies van de EDPB (artikel 64)

Advies 19/2024 over de EuroPrise-certificeringscriteria in verband met hun goedkeuring door het Comité als Europees gegevensbeschermingszegel krachtens artikel 42, lid 5 (AVG)

Vastgesteld op 16 juli 2024

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

Inhoudsopgave

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, en 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 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), 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 dat 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 de 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 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 een "Leidraad voor de

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

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, 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

1. In overeenstemming met artikel 42, lid 5, AVG en de richtsnoeren heeft de Duitse rechtspersoon EuroPrise Cert GmbH (hierna "de eigenaar van de regeling" genoemd) een ontwerpversie van de "EuroPrise-catalogus van criteria voor de certificering van verwerkingsactiviteiten door verwerkers (toepassingsgebied: EU), v1.5" (hierna "de ontwerpcertificeringscriteria", "de certificeringscriteria" of "de criteria" genoemd) opgesteld en voorgelegd aan de Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, de bevoegde Duitse toezichthoudende autoriteit in Noordrijn-Westfalen.

2. De nationale toezichthoudende autoriteit van Duitsland heeft de ontwerpcertificeringscriteria op 29 april 2024 ter goedkeuring voorgelegd aan het Comité overeenkomstig artikel 64, lid 2, AVG. De beslissing ten aanzien van de volledigheid van het dossier is genomen op 29 mei 2024.

3. Het EuroPrise-certificeringsmechanisme is geen certificering in de zin van artikel 46, lid 2, punt f), AVG 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. De doorgifte van persoonsgegevens naar een derde land of een internationale organisatie mag immers alleen plaatsvinden als de bepalingen van hoofdstuk V 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.

2.1 Toepassingsgebied van het certificeringsmechanisme en onderwerp van de beoordeling

5. Het EuroPrise-certificeringsmechanisme omvat certificeringscriteria uit een EU-brede certificeringsregeling voor de certificering van verwerkingsactiviteiten door verwerkers. Het voorwerp waarop de criteriacatalogus van toepassing is, bestaat in verwerkingsactiviteiten die worden uitgevoerd in het kader van producten, processen en diensten of met behulp van (verschillende) producten en diensten ten aanzien waarvan de aanvrager van de certificering als verwerker optreedt. De belangrijkste criteria van dit certificeringsmechanisme zijn onderverdeeld in drie reeksen vereisten, namelijk vanuit juridisch oogpunt (reeks 1), vanuit het oogpunt van technische en organisatorische maatregelen (reeks 2) en vanuit het oogpunt van de rechten van de betrokkenen (reeks 3).

6. Aanvragers van certificering in het kader van deze regeling moeten verwerkers zijn. Hiertoe behoren ook verwerkers die rechtstreeks zijn belast met de verwerking van persoonsgegevens door een verwerkingsverantwoordelijke in de zin van artikel 4, lid 7, AVG. Certificeringsaanvragers kunnen echter ook verwerkers zijn in de zin van artikel 28, leden 2 en 4, AVG (d.w.z. subverwerkers).

7. Wanneer een – krachtens de EuroPrise-certificeringsregeling gecertificeerde – verwerker een beroep doet op een subverwerker, kan die subverwerker niet stellen over een EuroPrise-certificering te

beschikken. In een dergelijke situatie vallen alleen de verwerkingsactiviteiten die worden uitgevoerd door de oorspronkelijke gecertificeerde verwerker onder de certificering. Subverwerkers kunnen echter ook zelf een certificering aanvragen, wat dan leidt tot een afzonderlijke, onafhankelijke procedure.

8. Het Comité leest in de door de Duitse toezichthoudende autoriteit verstrekte documentatie over het toepassingsgebied van het certificeringsmechanisme dat de EuroPrise-regeling van toepassing is op verwerkers die gevestigd zijn in de Europese Unie (EU) of in de Europese Economische Ruimte (EER).

2.2 Verwerkingsactiviteiten

9. Het toepassingsgebied van deze criteria is niet beperkt tot bepaalde soorten verwerkingsactiviteiten. Het gaat veeleer om de methodologie die ten grondslag ligt aan de EuroPrise-beoordeling, die het mogelijk maakt om alle door verwerkers verrichte verwerkingshandelingen te certificeren. Dit vormt dus een universele methodologische benadering op basis waarvan een groot aantal zeer uiteenlopende verwerkingsactiviteiten kan worden gecertificeerd. Daarom is het van fundamenteel belang dat aan de methodologische vereisten wordt voldaan; dit is immers de enige manier om een uniforme toepassing van de certificeringscriteria en een vergelijkbaar beproevingsniveau in de verschillende certificeringsprocedures te waarborgen. Het doel bestaat erin om de vergelijkbaarheid en reproduceerbaarheid van de toegekende certificeringen en de resultaten daarvan te garanderen.

2.3 Rechtmatigheid en beginselen van gegevensverwerking

10. De criteria vereisen dat er wordt nagegaan of de te certificeren verwerkingsactiviteiten voldoen aan de beginselen van gegevensbescherming door ontwerp en door standaardinstellingen (afdeling 1.5 van de criteria), wat inhoudt dat de aanvrager de verwerkingsverantwoordelijke bijstaat bij de tenuitvoerlegging van deze beginselen. Daardoor kan de naleving van artikel 25 AVG, gelezen in samenhang met artikel 5 AVG, worden beoordeeld. Hoewel geen van de criteria rechtstreeks gericht is op de naleving van artikel 6 AVG – aangezien de verwerkingsverantwoordelijke verantwoordelijk is voor de rechtmatigheid van de verwerking – hebben de criteria tot doel ervoor te zorgen dat verwerkers die certificering aanvragen de te certificeren verwerkingsactiviteiten zodanig opzetten dat de verwerkingsverantwoordelijken de gegevensbeschermingsbeginselen van artikel 5 AVG, met inbegrip van het beginsel van rechtmatigheid van de verwerking, gemakkelijker kunnen toepassen.

2.4 Algemene verplichtingen van verwerkingsverantwoordelijken en verwerkers

11. De criteria weerspiegelen de verhouding tussen de verwerker en de verwerkingsverantwoordelijke. Zij voorzien met name in een verplichting voor de verwerker om te beschikken over een model voor een gegevensverwerkingsovereenkomst met de verwerkingsverantwoordelijke, waarin alle vereisten van artikel 28 AVG zijn opgenomen (afdeling 1.2 van de criteria).

12. Op grond van de criteria moeten aanvragers een functionaris voor gegevensbescherming aanstellen overeenkomstig artikel 37 AVG en daar bewijs van overleggen (bijv. een aanstellingscertificaat). Via de criteria wordt nagegaan of de functionaris voor gegevensbescherming voldoet aan de vereisten van de artikelen 37 tot en met 39 (reeks 1, afdeling 1.1 van de criteria).

13. De criteria strekken ook tot controle van de inhoud van registers van verwerkingsactiviteiten overeenkomstig artikel 30 AVG (reeks 1, afdeling 1.1 van de criteria).

2.5 Rechten van de betrokkenen

14. In de criteria komt het recht van de betrokkene op informatie overeenkomstig hoofdstuk III 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 correctie, wissing of beperking mogelijk te maken (reeks 3 van de criteria).

2.6 Risico's voor de rechten en de vrijheid

15. Volgens de criteria moet de verwerker zich bewust zijn van de mogelijke risico's voor de rechten en vrijheden van natuurlijke personen die gepaard gaan met de gegevensverwerking in het kader van het onderwerp van de beoordeling. Indien de verwerking van persoonsgegevens waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen oplevert, zorgen verschillende criteria ervoor dat de aanvrager moet aantonen dat aan de vereisten van artikel 35 AVG is voldaan (punt 1.2.2 van de criteria, vereiste nr. 6, punt 1.3.2 van de criteria, punt 1.3.3 van de criteria, paragraaf 2.1.5.1 van de criteria, paragraaf 2.1.5.9 van de criteria).

2.7 Technische en organisatorische maatregelen ter waarborging van de bescherming

16. De criteria vereisen de toepassing van technische en organisatorische maatregelen die de vertrouwelijkheid, integriteit en beschikbaarheid van de verwerkingsactiviteiten 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 (afdeling 1.5 van de criteria, afdeling 2.1 van de criteria/overige documenten).

17. 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 artikel 33 AVG (punt 1.2.2 van de criteria, vereiste nr. 6).

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

18. Volgens de criteria moeten alle doorgiften van persoonsgegevens naar derde landen en naar internationale organisaties die bij het onderwerp van de beoordeling betrokken zijn worden geïdentificeerd en moet de gemaakte keuze met betrekking tot het mechanisme voor gegevensdoorgifte met passende waarborgen worden gemotiveerd, overeenkomstig hoofdstuk V AVG (afdeling 1.4 van de criteria).

3. AANVULLENDE CRITERIA VOOR EEN EUROPEES GEGEVENSBESCHERMINGSZEGEL

19. 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". Op grond van deel 4 van de criteria moet de aanvrager de toepasselijke nationale en relevante sectorspecifieke wetgeving inzake gegevensbescherming naleven. Voorts begrijpt de EDPB dat er een "verslag over de naleving van het nationale recht" – waarin met name wordt beoordeeld of het onderwerp van de beoordeling in overeenstemming is met de toepasselijke nationale wetsvoorschriften inzake

gegevensbescherming – moet worden opgesteld door juridisch deskundigen, die blijk moeten geven van het vereiste expertiseniveau op het gebied van het toepasselijke nationale recht.

CONCLUSIES/AANBEVELINGEN

20. Concluderend is het Comité van oordeel dat de ontwerpcertificeringscriteria 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).

21. Het Comité zal het certificeringsmechanisme “EuroPrise-catalogus van criteria voor de certificering van verwerkingsactiviteiten door verwerkers” registreren in het openbaar register van certificeringsmechanismen en gegevensbeschermingszegels en -merktekens overeenkomstig artikel 42, lid 8.

SLOTOPMERKINGEN

22. Dit advies is gericht tot de Duitse toezichthoudende autoriteit in Noordrijn-Westfalen en wordt bekendgemaakt op grond van artikel 64, lid 5, punt b), AVG.

Voor het Europees Comité voor gegevensbescherming

De voorzitter
Anu Talus