Advies van de EDPB (artikel 64)

Advies 15/2023 inzake het ontwerpbesluit van de Nederlandse toezichthoudende autoriteit met betrekking tot de certificeringscriteria van Brand Compliance

Vastgesteld op 19 september 2023

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 1, punt c), 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, als gewijzigd bij Besluit nr. 154/2018 van het Gemengd Comité van de EER van 6 juli 2018[1],

Gezien artikel 64, lid 1, punt c), van de AVG en 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 "de EDPB" 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 invoering van certificeringen de transparantie versterken en betrokkenen in staat stellen het gegevensbeschermingsniveau van de betreffende producten en diensten te beoordelen[3].

(2) De certificeringscriteria maken integraal deel uit van certificeringsmechanismen. Bijgevolg wordt in de AVG de goedkeuring vereist van de nationale certificeringscriteria van een 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 de EDPB (artikel 42, lid 5, en artikel 70, lid 1, punt o), AVG).

(3) Wanneer een toezichthoudende autoriteit voornemens is een certificering goed te keuren uit hoofde van artikel 42, lid 5, AVG, is het de belangrijkste taak van de EDPB om door middel van het in de artikelen 63, 64 en 65 van de AVG bedoelde coherentiemechanisme te waarborgen dat de AVG consistent wordt toegepast. In dit kader moet de EDPB in overeenstemming met artikel 64, lid 1, punt c), AVG een advies uitbrengen over het ontwerpbesluit van de toezichthoudende autoriteit tot goedkeuring van de certificeringscriteria.

(4) Met dit advies wordt beoogd de consistente toepassing van de AVG, onder meer door de toezichthoudende autoriteiten, verwerkingsverantwoordelijken en verwerkers, te waarborgen met betrekking tot de kernelementen die certificeringsmechanismen moeten ontwikkelen. Meer specifiek wordt de beoordeling door de EDPB uitgevoerd op basis van de "Richtsnoeren 1/2018 betreffende certificering en het identificeren van certificeringscriteria

[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.

in overeenstemming met artikel 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 de EDPB 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 certificeringscriteria de in de AVG vastgestelde vereisten en beginselen inzake de bescherming van persoonsgegevens naar behoren weerspiegelen en bijdragen tot de consistente toepassing ervan.

(7) Tegelijkertijd moeten de certificeringscriteria rekening houden en, in voorkomend geval, interoperabel zijn met andere normen, zoals ISO-normen, en certificeringspraktijken.

(8) Bijgevolg moeten certificeringen een toegevoegde waarde hebben voor de organisatie door deze te helpen gestandaardiseerde en gespecificeerde organisatorische en technische maatregelen te treffen die de conformiteit van verwerkingsprocessen aantoonbaar vergemakkelijken en versterken, met inachtneming van sectorspecifieke behoeften.

(9) De EDPB verwelkomt de inspanningen die eigenaren van regelingen zich getroosten om praktische en potentieel kostenefficiënte certificeringsmechanismen te ontwikkelen die de coherentie met de AVG verbeteren en het recht op privacy en gegevensbescherming van betrokkenen te bevorderen door de transparantie te vergroten.

(10) De EDPB 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) Het advies van de EDPB zal overeenkomstig artikel 64, lid 1, punt c, van de AVG in samenhang met artikel 10, lid 2, van het reglement van orde van de 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. Die termijn kan door de voorzitter met zes weken worden verlengd, rekening houdend met de complexiteit van de aangelegenheid.

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

BRENGT HET VOLGENDE ADVIES UIT:

1 OVERZICHT VAN DE FEITEN

1. De "Brand Compliance-certificeringsnorm" (hierna "ontwerpcertificeringscriteria" of "certificeringscriteria" genoemd) werd overeenkomstig artikel 42, lid 5, AVG en de richtsnoeren opgesteld door Brand Compliance B.V. (hierna "Brand Compliance" genoemd), een juridische entiteit in Nederland, en ingediend bij de Nederlandse toezichthoudende autoriteit.

2. De Nederlandse toezichthoudende autoriteit heeft haar ontwerpbesluit tot goedkeuring van de Brand Compliance-certificeringscriteria op 26 april 2023 ingediend en verzocht om een advies van de EDPB uit hoofde van artikel 64, lid 1, punt c), AVG. Op 4 juli 2023 is beslist dat het dossier volledig was.

2 EVALUATIE

3. De EDPB heeft zijn beoordeling uitgevoerd in overeenstemming met de structuur waarin bijlage 2 bij de richtsnoeren (hierna "bijlage" genoemd) en het addendum bij deze richtsnoeren voorzien. Indien in dit advies niet wordt ingegaan op een specifieke afdeling van de ontwerpcertificeringscriteria van Brand Compliance, moet worden verondersteld dat de EDPB geen opmerkingen heeft en de Nederlandse toezichthoudende autoriteit niet verzoekt nadere actie te ondernemen.

4. Deze certificering is geen certificering in de zin van artikel 46, lid 2, punt f), AVG die 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.

2.1. ALGEMENE OPMERKINGEN

5. In het algemeen wijst de EDPB erop dat diverse criteria te algemeen verwoord zijn, waardoor verwarring kan ontstaan omtrent wat geaccrediteerde certificeringsorganen moeten controleren en hoe. De EDPB is met name van mening dat bepaalde criteria niet reproduceerbaar en consistent kunnen worden beoordeeld door verschillende geaccrediteerde certificeringsorganen. Zo kan in afdeling 6.1.2.b bijvoorbeeld niet duidelijk van het criterium worden afgeleid hoe het certificeringsorgaan controleert of de aanvrager heeft voldaan aan de voorwaarden voor ondubbelzinnige toestemming. In dit opzicht is de EDPB van mening dat de aanvrager niet alleen een verklaring moet verstrekken waarin hij aangeeft de ondubbelzinnige aard van toestemming te eerbiedigen, maar ook bewijsmateriaal moet verstrekken van een ondubbelzinnige actieve handeling van de betrokkenen (bv. het aanvinken van selectievakjes die niet van tevoren aangevinkt waren, schriftelijke of mondelinge verklaring, een online proactieve handeling van de betrokkene enz.), alsmede bewijs van de invoering van een procedure die garandeert dat de toestemming wordt toegepast conform de beslissing (bv. vraaggesprekken met betrokkenen, resultaten van door de verwerkingsverantwoordelijke uitgevoerde testpanels enz.). De EDPB beveelt derhalve aan elk certificeringscriterium zo vorm te geven dat verschillende certificeringsorganen deze consistent en reproduceerbaar kunnen beoordelen.

   Dit geldt onder meer voor de criteria die hieronder worden vermeld:

   - in afdeling 5.3.2 ("*Data Protection Officer (DPO)*" [functionaris voor gegevensbescherming (DPO)]), de criteria waarmee kan worden aangetoond dat de DPO over deskundige kennis over gegevensbescherming en -praktijken beschikt (afdeling 5.3.2.1.b), tijdig wordt geraadpleegd (afdeling 5.3.2.2.a) en actieve steun

geniet van de raad van bestuur (afdeling 5.3.2.2.b), en dat de interne organisatie op de hoogte is van het bestaan van de DPO (afdeling 5.3.2.2.d);

- in afdeling 6.1.2 ("*lawfulness*" [rechtmatigheid]), de criteria in verband met de rechtmatigheid van de verwerking, bijvoorbeeld de manier waarop de organisatie kan aantonen dat in de praktijk wordt voldaan aan de voorwaarden voor toestemming (afdeling 6.1.2.b) of dat met de verwerking een gerechtvaardigd belang wordt nagestreefd met betrekking tot de rechten en vrijheden van de betrokkenen (afdeling 6.1.2.g);
- in afdeling 6.2.3 ("*data minimisation*" [gegevensminimalisatie]), het criterium dat informatie moet worden verstrekt over de verschillende mogelijke verwerkingsscenario's waar de organisatie van uitgaat.

6. De EDPB wijst erop dat de ontwerpcertificeringscriteria van Brand Compliance op grond van artikel 43, lid 6, AVG, door de toezichthoudende autoriteit in een toegankelijk formaat openbaar moeten worden gemaakt. Derhalve pleit de EDPB ervoor de verklaring inzake auteursrechten in dit document te wijzigen om te verduidelijken dat het document overeenkomstig artikel 43, lid 6, AVG openbaar zal worden gemaakt door de toezichthoudende autoriteit.

7. Hoewel in de inleiding van de ontwerpcertificeringscriteria wordt aangegeven dat Brand Compliance een nationaal certificeringsmechanisme is in de zin van artikel 42, lid 5, eerste zin, AVG, is de EDPB van mening dat het nationale toepassingsgebied van de criteria niet geheel duidelijk naar voren komt in de criteria. De EDPB merkt in het bijzonder op dat de ontwerpcertificeringscriteria meerdere verwijzingen bevatten naar de "wetgeving" en "aanvullende vereisten" van lidstaten, bijvoorbeeld in de afdelingen 5, 6, 7 en 8, en naar de effecten van verwerkingsactiviteiten op betrokkenen in meer dan één lidstaat, bijvoorbeeld in de afdelingen 6.1.2.c en 8.2.1 van de regeling. Volgens de EDPB kan dit tot verwarring leiden omtrent het toepassingsgebied van de certificeringscriteria. Daarom adviseert de EDPB te verduidelijken dat Brand Compliance een nationale certificeringsregeling is[4].

8. De EDPB merkt op dat er in de inleiding op wordt gewezen dat de organisatie moet voldoen aan alle certificeringscriteria van Brand Compliance, tenzij zij kan aantonen dat de uitsluitingen geen afbreuk doen aan haar vermogen om de AVG en deze norm na te leven ("*unless [it] can demonstrate that the exclusions have no impact on the organisations ability to comply with the GDPR and this Standard*"). Daarbij beklemtoont de EDPB dat de aanvrager geen van de criteria die zijn opgenomen in de certificeringsregeling eenvoudigweg naast zich neer mag leggen, zelfs niet als de aanvrager beweert te kunnen aantonen op een andere manier aan de AVG te voldoen. In sommige gevallen kan de aanvrager beoordelen of bepaalde criteria toepasselijk zijn, bijvoorbeeld met het oog op de reikwijdte van het onderwerp van beoordeling of de toepasbaarheid van specifieke vereisten uit hoofde van de AVG (zoals de benoeming van een DPO), maar in die gevallen moeten deze criteria worden geëvalueerd door de aanvrager en moet die evaluatie vervolgens worden gecontroleerd door het certificeringsorgaan. Derhalve adviseert de EDPB deze zin uit de ontwerpcertificeringscriteria te schrappen.

[4] Zie artikel 42, lid 4, en de artikelen 55 en 56 van de AVG.

9. De EDPB merkt op dat de terminologie in de naam van de certificeringscriteria misleidend kan zijn, aangezien hierin "*certification standard*" (certificeringsnorm) wordt gebruikt, in plaats van "*criteria*", als in artikel 42, lid 5, en artikel 64, lid 1, punt c), AVG. Derhalve pleit de EDPB ervoor het woord "*standard*" (norm) overal in het document te vervangen door "*criteria*".

10. De EDPB adviseert de betekenis van sommige termen in afdeling 3.1 ("*Terminology*" [Terminologie]) te verduidelijken door in voorkomend geval te verwijzen naar de overeenkomstige definitie in artikel 4 AVG. De EDPB pleit er bijvoorbeeld voor om, in plaats van te verklaren dat een begrip de betekenis heeft die wordt vermeld in de AVG (''*the term has the meaning as set out in the GDPR*''), rechtstreeks te verwijzen naar de definities in artikel 4, punt 7, voor "*controller*" (verwerkingsverantwoordelijke), artikel 4, punt 8, voor "*processor*" (verwerker), artikel 4, punt 11, voor "*consent*" (toestemming) en artikel 4, punt 12, voor "*personal data breach*" (inbreuk in verband met persoonsgegevens).

11. Daarnaast neemt de EDPB nota van de definitie van "*requirement*" (vereiste) in afdeling 3.1 ("*Terminology*" [Terminologie]) als "*rule or legal obligation, agreement, need or legitimate expectation regarding the target of evaluation*" (regel of wettelijke verplichting, overeenkomst, noodzaak of legitieme verwachting met betrekking tot het onderwerp van beoordeling). De EDPB is echter van mening dat het onduidelijk is of de gebruikte termen "*requirement*" (vereiste) in de afdelingen 4.2 en 5.2.1 en "*internal and external requirement*" (interne en externe vereiste) in de afdelingen 3.1, 7.2.e, 7.2.f en 9.2.1.b verwijzen naar technische en organisatorische maatregelen (TOM) of naar aanvullende doelstellingen inzake gegevensbescherming. Derhalve pleit de EDPB ervoor de definitie en het gebruik van het begrip "*requirement*" (vereiste) in de ontwerpcertificeringscriteria te verduidelijken.

12. Omwille van de consistentie beveelt de EDPB ook aan de in de vereisten gebruikte terminologie af te stemmen op de terminologie uit de AVG. Dit geldt met name voor de volgende begrippen:
    - in afdeling 6.1.2.b, punt c), van de certificeringscriteria moet de zinsnede "*can be freely given*" (kan vrijelijk worden gegeven) worden vervangen door "*is freely given*" (wordt vrijelijk gegeven);
    - in afdeling 6.1.3.b worden in de certificeringscriteria de begrippen "*intake*" (ontvangst) en "*scope*" (reikwijdte) van persoonsgegevens gebruikt, terwijl in de AVG wordt gesproken over de "*collection of personal data*" (verzameling van persoonsgegevens);
    - in afdeling 6.1.4.c moeten de zinsneden "*further processing*" (verdere verwerking)" en "*not further processed*" (niet verder verwerkt) worden gebruikt in plaats van respectievelijk "*repeated use of personal data*" (herhaaldelijk gebruik van persoonsgegevens) en "*frozen*" (bevroren);
    - In afdeling 8.6.g moet het begrip "*consent*" (toestemming) worden vervangen door "*authorisation*" (toestemming) in overeenstemming met artikel 28, lid 2, AVG;
    - in de afdelingen 8.4.8.b en 8.4.8.c. moet het begrip "[…] *fully automated individual decision making*" (volledig geautomatiseerde individuele besluitvorming) worden vervangen door "[…] *decision based solely on automated processing*" (uitsluitend op geautomatiseerde verwerking gebaseerd besluit) in overeenstemming met artikel 22, lid 1, AVG;
    - in afdeling 8.4 wordt verwezen naar "*the right to restrict processing*" (het recht om verwerking te beperken) in plaats van naar het "*right to restriction of processing*" (recht op beperking van de verwerking).

13. De nummering van afdelingen en verwijzingen naar andere afdelingen van de certificeringscriteria zijn soms onnauwkeurig (bv. noot 2 in afdeling 6.1.2.d, afdeling 6.1.5, afdeling 6.4, afdeling 6.5, afdeling 7.4.a). De EDPB adviseert derhalve de nummering van deze afdelingen dienovereenkomstig te rectificeren.

2.2 TOEPASSINGSGEBIED VAN HET CERTIFICERINGSMECHANISME EN ONDERWERP VAN BEOORDELING

14. De EDPB neemt nota van het feit dat afdeling 4 criteria bevat voor de vaststelling van het onderwerp van beoordeling (target of evaluation, ToE). Met name in afdeling 4.2.a zijn criteria opgenomen aan de hand waarvan de organisatie de toepasbaarheid van de AVG kan bepalen en documenteren, en wordt aangegeven dat de uitsluiting van uitvoeringscriteria moet worden gerechtvaardigd ("*exclusion of implementation criteria shall be justified*"). In dit opzicht wijst de EDPB erop dat het certificeringsorgaan en niet de aanvrager beslist of een specifiek criterium wel of niet moet worden toegepast. Derhalve adviseert de EDPB deze zin uit de ontwerpcertificeringscriteria te schrappen.

15. De EDPB merkt op dat in de certificeringscriteria niet duidelijk wordt aangegeven of subverwerkers via de regeling kunnen worden gecertificeerd. De certificeringscriteria bevatten met name geen specifieke criteria voor subverwerkers. Als een subverwerker zich voor de regeling aanmeldt, is de EDPB van mening dat afdeling 8.6 niet van toepassing is. Een voorbeeld: in een relatie van subverwerking voert een subverwerker die certificering aanvraagt verwerkingsactiviteiten uit in opdracht van een verwerker en kan hij derhalve niet per definitie aantonen dat de ontvangen instructies afkomstig zijn van de verwerkingsverantwoordelijke, zoals wordt geopperd in afdeling 8.6. Een subverwerker moet derhalve een specifieke verplichting hebben om de verwerker te informeren, die anders is dan de informatieverplichting in afdeling 8.6.c. Bovendien zou afdeling 8.8.4 bij een inbreuk op gegevens niet toepasbaar zijn en moeten er specifieke aangepaste criteria komen voor de certificering van subverwerkers, op grond waarvan de subverwerker de verwerker in kennis moet stellen. Indien subverwerkers in aanmerking komen voor certificering, adviseert de EDPB specifieke criteria te ontwikkelen om rekening te houden met de specifieke kenmerken van subverwerking. Als dit niet het geval is, adviseert de EDPB uitdrukkelijk te vermelden in de inleiding dat subverwerkers niet kunnen worden gecertificeerd via de Brand Compliance-certificeringsregeling en zo duidelijk te maken dat zij buiten het toepassingsgebied van deze regeling vallen.

16. De certificeringscriteria maken deel uit van een algemene certificeringsregeling in de zin van artikel 42, lid 5, AVG, die wordt toegepast in Nederland, en is derhalve niet gericht op een specifieke sector of een specifiek type verwerkingsactiviteiten. Volgens de verstrekte informatie bestaat de doelgroep uit organisaties in hun rol als verwerkingsverantwoordelijke of verwerker, ongeacht hun aard, omvang of de verwerking die plaatsvindt in het kader van de producten en diensten die zij leveren ("*in their role as controllers or processors, regardless of their type, size or the processing carried out in the framework of the products and services they provide*"). De EDPB is van mening dat het toepassingsgebied verder moet worden verduidelijkt door te verwijzen naar verwerkingsverantwoordelijken, verwerkers, gezamenlijke verwerkingsverantwoordelijke (en, in voorkomend geval, subverwerkers)

("*controllers, processors, joint controllers [and, if applicable, sub-processors*][5]"), alsmede naar het type producten en diensten ("*type of product and services*") dat zij leveren, en adviseert de inleiding dienovereenkomstig te wijzigen.

17. De EDPB merkt op dat afdeling 4 geen specifieke criteria bevat met betrekking tot de aanwijzing van alle gegevensverwerkingsactiviteiten die binnen het toepassingsgebied van de certificering vallen tijdens de vaststelling van het ToE. De EDPB beklemtoont dat de omschrijving van het ToE ook details moet bevatten over de rol van de spelers die zijn betrokken bij de verwerkingsactiviteiten (bv. verwerkingsverantwoordelijke, verwerker, gezamenlijke verwerkingsverantwoordelijke), alsmede informatie over potentiële gegevensdoorgifte aan landen buiten de EU/EER. De EDPB begrijpt dat sommige van deze criteria zijn uitgewerkt in de afdelingen 4.2 en 4.3, maar beveelt echter aan te verduidelijken dat deze criteria in een vroeg stadium, wanneer het ToE overeenkomstig afdeling 4.1 wordt vastgesteld, beoordeeld moeten worden.

18. In afdeling 4.3 wordt in de certificeringscriteria gesteld dat het de plicht van de aanvrager is om het toepassingsgebied van de certificering te bepalen. Eveneens wordt in het criterium in afdeling 4.3.c gesteld dat het de taak van het management van de aanvrager is om het ToE en het toepassingsgebied van de certificering goed te keuren. De EDPB beklemtoont dat de rol van de aanvrager bestaat uit het exact omschrijven in de aanvraag voor certificering van het beoogde toepassingsgebied van de certificering en het ToE, zodat deze vervolgens kunnen worden geëvalueerd door een certificeringsorgaan. Het is echter niet de taak van de aanvrager om het toepassingsgebied van de criteria te valideren. De rol van de aanvrager is beperkt tot het omschrijven en voorstellen van het toepassingsgebied van het certificeringsmechanisme en het ToE, en het certificeringsorgaan moet vervolgens beslissen of de aanvrager in aanmerking komt voor certificering. De EDPB adviseert te verduidelijken dat het aan het certificeringsorgaan is om een besluit te nemen over de vaststelling van het toepassingsgebied van de certificering en het ToE nadat deze door de aanvrager zijn voorgesteld en omschreven.

19. In afdeling 5.3.2.1.d pleit de EDPB ervoor te verduidelijken dat de organisatie de DPO moet registreren bij de Nederlandse toezichthoudende autoriteit gezien het nationale toepassingsgebied van de certificeringscriteria.

2.3 RECHTMATIGHEID VAN VERWERKING

20. De EDPB merkt op dat in afdeling 6.1.2 ("*Lawfulness*" [Rechtmatigheid]) wordt gesteld dat de organisatie moet bepalen of verwerking is toegestaan door na te gaan of is voldaan aan ten minste een van de volgende voorwaarden voor rechtmatigheid ("*determine that processing is allowed because at least one of the following conditions [for lawfulness] have been met*"). In dit opzicht is de EDPB van mening dat in de ontwerpcertificeringscriteria duidelijk moet worden gemaakt dat er van de rechtsgrondslagen die worden vermeld in artikel 6 AVG maar één rechtsgrondslag hoeft te worden gekozen waaraan moet worden voldaan. Daarnaast is de EDPB van mening dat in de certificeringscriteria het vereiste moet worden opgenomen om de toepasbaarheid en, indien relevant, geschiktheid van de rechtsgrondslag aan te tonen, met inachtneming van de verwerkingsactiviteiten en afhankelijk van de aard, omvang, context en

[5] Zie de aanbeveling in punt 15 van dit advies.

doeleinden van de verwerking. De EDPB adviseert derhalve afdeling 6.1.2 dienovereenkomstig te wijzigen.

21. De EDPB merkt op dat sommige criteria met betrekking tot toestemming in de afdelingen 6.1.2.b en 8.3.1.1.b herhaald worden. Voor de duidelijkheid pleit de EDPB ervoor duidelijke verbanden te leggen tussen de criteria in plaats van ze te herhalen. Daarnaast beveelt de EDPB aan in afdeling 6.1.2. b ("*Consent*" [Toestemming]) een vereiste toe te voegen met betrekking tot de toestemming van kinderen (bijvoorbeeld door te verwijzen naar afdeling 8.3.1.1 in afdeling 6.1.2.c), aangezien de voorwaarden die van toepassing zijn op de toestemming van kinderen met betrekking tot diensten van de informatiemaatschappij, ook een van de voorwaarden vormen om te waarborgen dat verwerking rechtmatig is.

22. De EDPB merkt op dat afdeling 6.1.2.c ("*performance of the contract*" [uitvoering van de overeenkomst]) het vereiste bevat dat de verwerking verband moet houden met de verwezenlijking van het hoofddoel van de overeenkomst en niet met verwante belangen van de organisatie ("*to be related to the achievement of the main purpose of the contract, and not to any related interests of the organisation*"). De EDPB pleit ervoor deze zin te verduidelijken door te stellen dat met de verwerking niet verder mag worden gegaan dan het doeleinde dat integraal deel uitmaakt van de uitvoering van de overeenkomst.

23. Met betrekking tot afdeling 6.1.2.h en onder verwijzing naar de artikelen 9 en 10 AVG, adviseert de EDPB uitdrukkelijk te verwijzen naar de voorwaarden in deze artikelen op grond waarvan het verbod niet geldt.

2.4 BEGINSELEN VAN ARTIKEL 5

24. Met betrekking tot afdeling 6.1 ("*Principles relating to the processing activities*" [Beginselen met betrekking tot de verwerkingsactiviteiten]), merkt de EDPB op dat het gebruik van de zinsnede "*principles of the GDPR*" (beginselen van de AVG) verwarrend kan zijn en pleit het ervoor specifieker te verwijzen naar "*principles in article 5 GDPR*" (beginselen in artikel 5 AVG).

25. Daarnaast merkt de EDPB op dat in afdeling 6.1.a ("*Policy regarding the principles*" [Beleid inzake de beginselen]) wordt bepaald dat de DPO moet worden geraadpleegd over de juiste toepassing van de beginselen in het geval van nieuwe verwerkingsactiviteiten en substantiële wijzigingen in bestaande verwerkingsactiviteiten. De EDPB merkt echter op dat raadpleging van de DPO niet moet worden beperkt tot deze gevallen. Naar de mening van de EDPB moet de DPO in voorkomend geval ook worden geraadpleegd om de toereikendheid te beoordelen van het beleid dat wordt vastgesteld inzake de toepassing van deze beginselen overeenkomstig afdeling 5.2.1.a. De EDPB pleit ervoor de rol van de DPO in verband met deze beginselen dienovereenkomstig te verduidelijken.

26. De EDPB merkt op dat in afdeling 6.1.1. van de certificeringscriteria te lezen is dat verdere verwerking voor archivering in het algemeen belang, voor wetenschappelijk of historisch onderzoek of statistische doeleinden niet wordt verondersteld onverenigbaar te zijn met de oorspronkelijke doeleinden ("*further processing for archiving in the general interest, for scientific or historic research, or statistical purposes is not considered to be incompatible with to the original purposes*"). De EDPB beveelt aan te verduidelijken dat verdere verwerking voor archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden niet *per definitie* wordt verondersteld in strijd te zijn met het oorspronkelijke doeleinde (enkelvoud), mits de beoordeling van de compatibiliteit van doeleinden naar behoren wordt gedocumenteerd, in het bijzonder met betrekking tot het bestaan van

passende waarborgen voor de rechten en vrijheden van de betrokkene[6]. De EDPB is met name van mening dat de passende waarborgen voor de rechten en vrijheden van betrokkenen die zijn ingevoerd voor elke verwerkingsactiviteit die wordt uitgevoerd voor doeleinden van archivering in het algemeen belang, voor wetenschappelijk of historisch onderzoek of voor statistische doeleinden, ook moeten worden gedocumenteerd door de organisatie en worden beoordeeld in het kader van de toetsing van verenigbaarheid waarnaar wordt verwezen in afdeling 6.1.1.c, punt 3 (i), (ii) en (iii). Dienovereenkomstig beveelt de EDPB aan in dit opzicht een specifiek criterium toe te voegen aan afdeling 6.1.1.c, punt 3 (i), (ii) en (iii).

27. De EDPB pleit ervoor de vereisten in afdeling 6.1.1.d ("*Necessity, proportionality and subsidiarity*" [Noodzaak, evenredigheid en subsidiariteit]) te verduidelijken, in het bijzonder hun verband met de beginselen uit artikel 5 AVG, evenals hun wisselwerking met de criteria in verband met de vaststelling van een rechtsgrond.

28. Met betrekking tot afdeling 6.1.1.1 ("*Transfer of personal data to a third party*" [Doorgifte van persoonsgegevens aan derden]) pleit de EDPB ervoor om, teneinde verwarring te voorkomen met de notie van internationale doorgifte van persoonsgegevens uit hoofde van hoofdstuk V, het begrip "*data transfer*" (gegevensdoorgifte) te vervangen door "*data sharing*" (gegevensuitwisseling) of "*data transmission*" (gegevensoverdracht).

29. Met betrekking tot afdeling 6.4.1 "*Data minimisation*" [Gegevensminimalisatie] beveelt de EDPB aan in overeenstemming met overweging 39 te verduidelijken dat het beginsel van gegevensminimalisatie in het bijzonder vereist dat wordt gewaarborgd dat de termijn dat persoonsgegevens worden bewaard, tot een strikt minimum wordt beperkt. Met betrekking tor afdeling 6.1.4.b ("*Accuracy with repeated use*" [Nauwkeurigheid bij herhaaldelijk gebruik]) beveelt de EDPB aan het vereiste van een "*longer period of time*" (langere periode) te verduidelijken zodat de aanvrager objectief kan beoordelen of hij voldoet aan deze criteria.

30. In afdeling 6.1.5. ("*Storage limitation*" [Beperking van bewaring]) beveelt de EDPB aan de verplichting voor de organisaties op te nemen om te garanderen dat de verwerkers met wie de gegevens zijn gedeeld of aan wie ze zijn overgedragen, de gegevens wissen, in overeenstemming met artikel 28, lid 3, punt g), AVG. Daarnaast beveelt de EDPB aan de zinsnede in afdeling 6.1.5.a waarin wordt gesteld dat de bewaartermijn onbeperkt kan zijn ("*the retention period [...] may be indefinite*") te schrappen, aangezien de bewaartermijn voor persoonsgegevens in alle gevallen moet worden vastgesteld. Met betrekking tot afdeling 6.1.5.c ("*Anonymisation*" [Anonimisering]) moedigt de EDPB de regelingbeheerders aan ook een verwijzing op te nemen naar gevallen waarin anonimisering plaatsvindt voor statistische en onderzoeksdoeleinden in overeenstemming met artikel 89, lid 1, AVG. Tot slot merkt de EDPB op dat er ook andere situaties zijn waarin gegevens gewist moeten worden, bijvoorbeeld wanneer de toezichthoudende autoriteit opdracht geeft tot het wissen van persoonsgegevens uit hoofde van artikel 58, lid 2, punt g), AVG, en pleit ervoor dit in de criteria op te nemen.

2.5. ALGEMENE VERPLICHTINGEN VOOR VERWERKINGSVERANTWOORDELIJKEN EN VERWERKERS

[6] Zie overweging 156 en artikel 89, lid 1, van de AVG.

31. De EDPB merkt op dat afdeling 6.2.a ("*Assessing the processing instructions*" [De verwerkingsinstructies beoordelen]) verkeerd kan worden geïnterpreteerd omdat de zin "*the organisation shall, where possible given the nature of the processing operation, establish, document and implement a process […]"* (de organisatie zal, indien mogelijk gezien de aard van de verwerkingsactiviteit, een proces opzetten, documenteren en invoeren […]) de indruk wekt dat de verwerker zelf kan beslissen of hij dit wel of niet doet. De EDPB beveelt derhalve aan "*where possible*" (indien mogelijk) te schrappen.

32. Met betrekking tot afdeling 6.5.1 ("*Joint controllers*" [Gezamenlijke verwerkingsverantwoordelijken]) merkt de EDPB op dat een verwerkingsverantwoordelijke tijdens het certificeringsproces van Brand Compliance een ToE kan indienen dat onderhevig is aan een gezamenlijke verwerkingsverantwoordelijkheid. De EDPB wil beklemtonen dat het geaccrediteerde certificeringsorgaan, als op het ToE een gezamenlijke verwerkingsverantwoordelijkheid rust, het aanvraagproces zorgvuldig moet uitvoeren om te garanderen dat het ToE betekenisvol is en dat de aanvrager volledig verantwoordelijk is voor de conformiteit van het ToE met alle verplichtingen op grond van de AVG die het certificeringsmechanisme beoogt aan te tonen. Als gevolg hiervan kan het zijn dat de aanvrager, vanwege de afspraken die zijn gemaakt tussen de aanvrager en de andere gezamenlijke verwerkingsverantwoordelijken die betrokken zijn bij het ToE met betrekking tot hun respectieve verantwoordelijkheden voor naleving van de verplichtingen uit hoofde van de AVG — afhankelijk van de context van de verwerkingsactiviteiten van het ToE — niet kan voldoen aan de criteria voor certificering. In dit opzicht wordt in afdeling 6.4.1.c ("*Evaluating the arrangements*" [De afspraken evalueren]) opgemerkt dat alle verwerkingsverantwoordelijken in dergelijke situaties gezamenlijk moeten worden gecertificeerd teneinde te waarborgen dat de certificering betekenisvol is voor de doelgroep ("*can only be certified as a whole in order to be meaningful to the target group*"). In dezelfde trant wordt in noot 3 van afdeling 4.3.a gesteld dat het ToE bij verwerkingsactiviteiten waarvoor verschillende partijen gezamenlijke verwerkingsverantwoordelijken zijn, de verwerkingsactiviteiten van de gezamenlijke verwerkingsverantwoordelijken moet beslaan ("*Processing operations for which several parties are joint controllers […] the ToE must cover the processing operations of the joint controllers*"). Het blijft echter onduidelijk wat dit als zodanig inhoudt voor het certificeringsproces. Derhalve beveelt de EDPB aan bij de vaststelling van het ToE te bepalen aan welke vereisten de afspraken moeten voldoen die worden gemaakt tussen de aanvrager en de andere gezamenlijke verwerkingsverantwoordelijken die betrokken zij bij het ToE inzake hun respectieve verantwoordelijkheden voor naleving van de Brand Compliance-certificeringscriteria. Daarnaast beveelt de EDPB aan in afdeling 6.4.1.b ("*Embedding the arrangements*" [De afspraken insluiten]) criteria op te nemen ter uitvoering van de bepalingen van artikel 26, lid 3, AVG.

33. Met betrekking tot afdeling 8.8.4 ("*Notification to the controller*" [Kennisgeving aan de verwerkingsverantwoordelijke]) pleit de EDPB ervoor de zin "*If and to the extent that it is not possible to provide the information at ones [once], it may be provided in stages without undue delay*" (Indien en voor zover het niet mogelijk is de informatie onmiddellijk te verstrekken, mag deze zonder onnodige vertraging gefaseerd worden verstrekt) opnieuw te formuleren om duidelijk te maken dat nog steeds alle noodzakelijke informatie moet worden verstrekt, zij het in een later stadium.

34. In afdeling 7.2.b ("*Risk management procedure*" [Procedure voor risicobeheer]) pleit de EDPB ervoor verwijzingen op te nemen naar afdeling 7.3 ("*DPIA and prior consultation*"[PEB en

raadpleging vooraf]) om ook aandacht te besteden aan gevallen waarvoor in de risicoanalyse en -evaluatie wordt geconcludeerd dat met verwerking nog steeds een hoog restrisico is gemoeid. Voorts adviseert de EDPB met betrekking tot de laatste zin van afdeling 7.2.b te verduidelijken dat de procedure moet waarborgen dat risicoanalyses, plannen voor de aanpak van risico's en restrisico's expliciet worden goedgekeurd door relevante directieleden.

35. Afdeling 8.7 ("*International transfer of personal data (where applicable)*" [Internationale doorgifte van persoonsgegevens, indien van toepassing]) bevat een uitgebreide lijst van hulpmiddelen die beschikbaar zijn voor doorgiften aan derde landen. In de afdeling wordt echter niet ingegaan op procedurele aspecten. De EDPB beveelt derhalve aan bepalingen toe te voegen over hoe er specifiek voor kan worden gezorgd dat de aanvrager in dat opzicht aantoont aan de AVG te voldoen.

36. De EDPB merkt op dat de verwijzing naar Aanbeveling 2/2020 van de EDPB in afdeling 8.7.c ("*Consulting the supervisory authority concerned*" [De betrokken toezichthoudende autoriteit raadplegen]) vrij algemeen is en pleit er derhalve voor te verduidelijken in welke omstandigheden toestemming vooraf van de desbetreffende toezichthoudende autoriteit vereist is.

2.6 RECHTEN VAN BETROKKENEN

37. In afdeling 8.2.2 ("*Providing information to the data subject*" [Verstrekken van informatie aan de betrokkene]) wordt verwezen naar vrijstellingen van de informatieplicht uit hoofde van artikel 14, lid 5, punt b), AVG. De EDPB merkt echter op dat hier een verwijzing ontbreekt naar het feit dat de verwerkingsverantwoordelijke, als het verstrekken van informatie onmogelijk is of een onevenredige inspanning zou vereisen, passende maatregelen moet nemen om de rechten en vrijheden en de legitieme belangen van de betrokken te beschermen, onder meer door de informatie openbaar te maken. De EDPB beveelt derhalve aan deze verwijzing op te nemen om afdeling 8.2.2 in overeenstemming te brengen met artikel 14, lid 5, punt b), AVG. Voorts beveelt de EDPB aan duidelijk onderscheid te maken tussen de vrijstellingen van de informatieplicht uit hoofde van artikel 13, lid 4, AVG en artikel 14, lid 5, punt b), AVG.

38. In afdeling 8.2.2.b ("*Preparing information to the data subjects*" [Informatie opstellen voor betrokkenen]) wordt gesteld dat over de informatie die wordt verstrekt aan de betrokkene, aantoonbaar overeenstemming moet worden bereikt met (de vertegenwoordigers van) die betrokkenen ("*the information provided to the data subject shall […] be demonstrably agreed with (the representatives of) the data subjects*"). De EDPB merkt echter op dat op grond van de AVG geen overeenstemming met een betrokkene nodig is over de informatie die wordt verstrekt overeenkomstig artikel 13 of artikel 14 AVG. Derhalve beveelt de EDPB aan in afdeling 8.2.2.b een andere bewoording te gebruiken teneinde misverstanden te voorkomen.

39. De EDPB merkt op dat de indruk wordt gewekt dat afdeling 8.4.1.d ("*Securing personal data (where applicable)*" [Persoonsgegevens beveiligen, indien nodig]) alleen van toepassing is wanneer persoonsgegevens gedurende een korte periode ("*for a short period of time*") worden bewaard. De EDPB is echter van mening dat een verwerkingsverantwoordelijke altijd de naleving moet waarborgen van de rechten die worden genoemd in hoofdstuk III van de AVG. Zo mag hij bijvoorbeeld persoonsgegevens niet opzettelijk wissen wanneer een

toegangsverzoek wordt ontvangen. Derhalve beveelt de EDPB aan het vereiste "*for a short period of time*" (gedurende een korte periode) te schrappen.

40. Met betrekking tot de afhandeling van verzoeken op grond van de rechten van betrokkenen wordt in afdeling 8.4.1.e ("*Handling of the rights of the data subjects*" [Afhandeling van verzoeken op grond van de rechten van betrokkenen]) gesteld dat dit per ommegaande en hoe dan ook binnen dertig dagen ("[…] *without undue delay and in no case later than 30 days*") moet gebeuren. In dit opzicht beveelt de EDPB aan in plaats daarvan de zinsnede "[…] *within one month of receipt of the request*" (binnen een maand na ontvangst van het verzoek) te gebruiken, in overeenstemming met artikel 12, lid 3, AVG.

41. In afdeling 8.4.2.b ("*Providing a copy*" [Een kopie verstrekken]) wordt bepaald dat de organisatie de betrokkene, naar aanleiding van een rechtmatig en uitvoerbaar verzoek, een kopie in een permanent formaat moet verschaffen van zijn of haar persoonsgegevens die door de organisatie zijn verwerkt ("*provides […] the data subject, upon lawful and executable request, with a copy in a permanent form of his or her personal data that was processed by the organization*"). Teneinde misverstanden en verschillende lezingen van deze bepaling te voorkomen, beveelt de EDPB aan in plaats daarvan te stellen dat de organisatie een kopie moet verschaffen van de persoonsgegevens die worden verwerkt ("[…] *provide a copy of the personal data undergoing processing*"), overeenkomstig de bepalingen van artikel 15, lid 3, AVG.

42. Met betrekking tot het recht op gegevenswissing wordt in afdeling 8.4.4.a gesteld dat de organisatie bepaalt en documenteert of en op welke voorwaarden het recht op gegevenswissing van toepassing is op de verwerkingsactiviteiten ("*The organisation shall determine and document whether and under what conditions the right of erasure applies to the processing activities*"). De EDPB pleit ervoor een verwijzing op te nemen naar artikel 17, lid 3, AVG om ook aandacht te besteden aan situaties waarin het recht op gegevenswissing niet van toepassing is, en deze naar behoren te documenteren.

43. De EDPB merkt op dat aan het begin van afdeling 8.4.6 ("*The right to data portability (where applicable)*" [Het recht op overdraagbaarheid van gegevens, indien van toepassing]) wordt gesproken over een verplichting voor de organisatie om dergelijke gegevens, als dat technisch haalbaar is, rechtstreeks over te dragen aan de beoogde ontvangen ("*[…] where technically feasible, transmit such data directly to the intended recipient*"). In dit opzicht beveelt de EDPB aan de bewoording "[…] *to another controller without hindrance*" (aan een andere verwerkingsverantwoordelijke, zonder daarbij te worden gehinderd) uit artikel 20, lid 1, AVG, te gebruiken om te verduidelijken dat met "*another controller*" (een andere verwerkingsverantwoordelijke) wordt verwezen naar de verwerkingsverantwoordelijke die is aangewezen door de betrokkene, en aan te geven dat het recht op overdraagbaarheid van gegevens ook van toepassing is op gegevens die zijn gegenereerd door de activiteiten van de betrokkene waar te nemen.

44. In afdeling 8.4.7 ("*The right to object*" [Het recht om bezwaar te maken]), wordt verwezen naar verwerking voor wetenschappelijke of historische doeleinden ("[…] *scientific or historical purposes*"). In dit opzicht beveelt de EDPB echter aan de bewoording "[…] *scientific or historical research purposes or statistical purposes*" (wetenschappelijk of historisch onderzoek of statistische doeleinden) uit artikel 21, lid 6, AVG te gebruiken.

45. De EDPB beveelt aan de titel van afdeling 8.4.8 ("*The right regarding automated decision-making*" [Het recht met betrekking tot geautomatiseerde besluitvorming]) te veranderen in

"*The right regarding automated individual decision-making, including profiling*" (Het recht met betrekking tot geautomatiseerde individuele besluitvorming, waaronder profilering), in overeenstemming met de titel van artikel 22 AVG. Daarnaast merkt de EDPB op dat in het gedeelte over "*objective*" (doel) wordt bepaald dat de organisatie moet garanderen dat geautomatiseerde individuele besluitvorming, waaronder profilering, nauwkeurig wordt uitgevoerd ("*ensure that automated individual decision making, including profiling, is carried out carefully*"). Aangezien het misschien niet mogelijk is de uitvoering daarvan in de praktijk te beoordelen, beveelt de EDPB aan het woord "*carefully*" (nauwkeurig) in deze paragraaf te schrappen.

46. Op grond van afdeling 8.4.8.f ("*Bias check*" [Vertekeningscontrole]) moet de organisatie ten minste een keer per jaar aantoonbaar systematische analyses uitvoeren om de nauwkeurigheid van het besluitvormingsproces te beoordelen en te bepalen of geen sprake is van vertekening (van resultaten), en moet zij het proces zo nodig aanpassen ("[…] *organisation shall demonstrably perform systematic analyses, at least annually, to determine the accuracy of the decision-making process and the absence of bias (distortion of results), and shall adjust the process as necessary.*"). De EDPB is van mening dat het niet volledig duidelijk is of "absence of bias" (geen sprake van vertekening) in afdeling 8.4.8.f wordt beschouwd als een aspect van de nauwkeurigheid van gegevens. De EDPB pleit er hoe dan ook voor om in afdeling 8.4.8.f een verwijzing op te nemen naar overweging 71 van de AVG om misverstanden te voorkomen, aangezien daar wordt ingegaan op de nauwkeurigheid van gegevens in het kader van profilering en van artikel 22 AVG.

47. In afdeling 8.4.10 wordt bepaald dat een organisatie als zij weigert een verzoek in te willigen, moet bewijzen dat het verzoek kennelijk ongegrond of buitensporig is ("[…] *the organisation refuses to comply with a request, it shall provide evidence that the request is manifestly unfounded or excessive*"). In tegenstelling tot hetgeen wordt bepaald in artikel 12, lid 5, AVG, kan in afdeling 8.4.10 onterecht de indruk worden gewekt dat het niet meer nodig zou zijn om dit aan te tonen als de verwerkingsverantwoordelijke redelijke kosten in rekening brengt voor de afhandeling van het verzoek van een betrokkene. Derhalve beveelt de EDPB aan duidelijk te maken dat in beide in artikel 12, lid 5, punten a) en b), AVG genoemde scenario's moet worden aangetoond dat het verzoek kennelijk ongegrond of buitensporig is.

48. Met betrekking tot afdeling 8.4.11 adviseert de EDPB te verduidelijk of met "*complaints procedure*" (klachtenprocedure) wordt verwezen naar processen voor geschillenbeslechting of naar formele klachten uit hoofde van artikel 77, lid 1, AVG.

2.7 RISICO'S VOOR DE RECHTEN EN VRIJHEDEN VAN NATUURLIJKE PERSONEN

49. De EDPB adviseert in afdeling 7.3a een verwijzing op te nemen naar de lijsten uit hoofde van artikel 35, leden 4 en 5, AVG, zoals gepubliceerd door de Nederlandse toezichthoudende autoriteit.

50. De laatste zin van afdeling 7.3.2 luidt als volgt: "[…] *or if the organisation develops processing operations under its own direction, comply with the requirements of Section 7.3 itself*." (of als de organisatie onder eigen regie verwerkingsactiviteiten ontwikkelt, zelf voldoen aan de vereisten van afdeling 7.3). De EDPB merkt op dat in situaties waarin een vermeende verwerker verwerkingsactiviteiten uitvoert onder eigen regie, de verwerker geen verwerker

zou zijn maar een verwerkingsverantwoordelijke. In dat geval zou afdeling 7.3.2 helemaal niet van toepassing zijn. Daarom beveelt de EDPB aan de laatste zin van afdeling 7.3.2 te schrappen.

2.8 TECHNISCHE EN ORGANISATORISCHE MAATREGELEN OM BESCHERMING TE GARANDEREN

51. De EDPB is van mening dat niet duidelijk is in welke mate het begrip "*controls*" (controles) waarnaar wordt verwezen in afdeling 7.2 ("*Risk management*" [Risicobeheer]) afwijkt van de notie van "*technical and organisational measures*" (technische en organisatorische maatregelen). De EDPB pleit ervoor dit punt dienovereenkomstig te verduidelijken.

55. De EDPB merkt op dat in afdeling 7.4 ("*Data protection by design and by default*" [Gegevensbescherming door ontwerp en door standaardinstellingen]) van de certificeringscriteria aandacht wordt besteed aan de verplichtingen in verband met gegevensbescherming door ontwerp en door standaardinstellingen uit hoofde van artikel 25 AVG, en pleit ervoor een verwijzing op te nemen naar de criteria voor verwerkers en subverwerkers die al zijn opgenomen in afdeling 8.2.5, zodat deze in acht worden genomen wanneer deze partijen in de arm worden genomen en bij de regelmatige evaluaties en beoordelingen van de activiteiten van verwerkers.

56. De EDPB pleit er eveneens voor te benadrukken dat verwerkers ernaar moeten streven gegevensbescherming door ontwerp en door standaardinstellingen te vergemakkelijken zodat de verwerkingsverantwoordelijke beter kan voldoen aan de verplichtingen uit hoofde van artikel 25.

57. Tot slot wordt in afdeling 7.5.1 ("*Competences*" [Competenties]) gesteld dat de organisatie in voorkomend geval stappen moet nemen om de nodige competenties te verwerven en de doeltreffendheid van de genomen stappen moet evalueren ("*where appropriate, take steps to acquire the necessary competence and evaluate the effectiveness of the steps taken*"). De EDPB is van mening dat altijd moet worden beoordeeld en gewaarborgd dat de personen die de gegevensverwerkingsactiviteiten uitvoeren over de vereiste competenties beschikken. De EDPB pleit er derhalve voor dit criterium dienovereenkomstig te wijzigen.

3 CONCLUSIES EN AANBEVELINGEN

Ter conclusie overweegt de EDPB het volgende:

Met betrekking tot de "algemene opmerkingen" adviseert de EDPB de Nederlandse toezichthoudende autoriteit om:

1. te garanderen dat elk certificeringscriterium in de volledige certificeringsregeling zo is vormgegeven dat verschillende certificeringsorganen deze consistent en reproduceerbaar kunnen beoordelen;
2. in de volledige certificeringsregeling te verduidelijken dat het toepassingsgebied nationaal is;

3. in het inleidende deel de zinsnede "*unless [it] "can demonstrate that the exclusions have no impact on the organisations ability to comply with the GDPR and this Standard*" (tenzij kan worden aangetoond dat de uitsluitingen geen afbreuk doen aan het vermogen van de organisaties om de AVG en deze standaard na te leven) te schrappen;
4. de in de vereisten van de volledige certificeringsregeling gebruikte terminologie af te stemmen op de terminologie van de AVG;
5. in de volledige certificeringsregeling de onnauwkeurige nummering van afdelingen en doorverwijzingen naar anderen afdelingen te corrigeren.

Met betrekking tot het "toepassingsgebied van het certificeringsmechanisme en het onderwerp van beoordeling" adviseert de EDPB de Nederlandse toezichthoudende autoriteit om:

1. in afdeling 4.2.a de zinsnede te schrappen dat de uitsluiting van uitvoeringscriteria gerechtvaardigd moet worden ("*exclusion of implementation criteria shall be justified*");
2. in de certificeringsregeling specifieke criteria op te nemen om rekening te houden met de specifieke kenmerken van subverwerking of in het inleidende deel aan te geven dat subverwerkers niet kunnen worden gecertificeerd via de certificeringsregeling;
3. de inleiding aan te passen om het toepassingsgebied verder te specificeren door te verwijzen naar verwerkingsverantwoordelijken, verwerkers, gezamenlijke verwerkingsverantwoordelijken (en, indien van toepassing, subverwerkers) ("*controllers, processors, joint controllers [and, if applicable, sub-processors*]"), alsmede het door hen geleverde type producten en diensten ("*type of product and services*");
4. in afdeling 4.1 te verduidelijken dat in een vroegtijdig stadium van de vaststelling van het ToE moeten worden bepaald welke gegevensverwerkingsactiviteiten binnen het toepassingsgebied van de certificering vallen;
5. in afdeling 4.3 te verduidelijken dat het aan het certificeringsorgaan is een besluit te nemen over de vaststelling van het toepassingsgebied van de certificering en het ToE nadat deze door de aanvrager zijn voorgesteld en omschreven.

Met betrekking tot de rechtmatigheid van verwerking adviseert de EDPB de Nederlandse toezichthoudende autoriteit om:

1. afdeling 6.1.2 te wijzigen om duidelijk te maken dat er maar één van de in artikel 6 AVG vermelde rechtsgronden hoeft te worden gekozen en nageleefd;
2. afdeling 6.1.2 te wijzigen om er het vereiste in op te nemen om de toepasbaarheid en, indien relevant, de geschiktheid van de rechtsgrondslag aan te tonen, met inachtneming van de verwerkingsactiviteiten en afhankelijk van de aard, omvang, context en doeleinden van de verwerking;
3. in afdeling 6.1.2.b een vereiste toe te voegen in verband met toestemming van kinderen;
4. in afdeling 6.1.2.h uitdrukkelijk te verwijzen naar de voorwaarden uit de artikelen 9 en 10 AVG.

Met betrekking tot "beginselen van artikel 5" adviseert de EDPB de Nederlandse toezichthoudende autoriteit om:

1. in afdeling 6.1.1 te verduidelijken dat verdere verwerking voor archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden niet *per definitie* wordt verondersteld in strijd te zijn met het oorspronkelijke doeleinde (enkelvoud), mits de beoordeling van de compatibiliteit van doeleinden naar behoren wordt gedocumenteerd, in het bijzonder met betrekking tot het bestaan van passende waarborgen voor de rechten en vrijheden van de betrokkene;

2. in afdeling 6.1.1.c, punt 3 (i), (ii) en (iii) een specifiek criterium toe te voegen op grond waarvan de passende waarborgen voor de rechten en vrijheden van betrokkenen die zijn ingevoerd voor elke verwerkingsactiviteit die wordt uitgevoerd voor doeleinden van archivering in het algemeen belang, voor wetenschappelijk of historisch onderzoek of voor statistische doeleinden, ook moeten worden gedocumenteerd door de organisatie en worden beoordeeld in het kader van de toets van verenigbaarheid waarnaar wordt verwezen in afdeling 6.1.1.c, punt 3 (i), (ii) en (iii);
3. in afdeling 6.4.1 te verduidelijken dat het beginsel van gegevensminimalisatie met name vereist dat ervoor wordt gezorgd dat de bewaartermijn van de persoonsgegevens tot een strikt minimum wordt beperkt;
4. in afdeling 6.1.4.b het vereiste van een "*longer period of time*" (langere periode) te verduidelijken zodat de aanvrager objectief kan beoordelen of hij aan dit criterium voldoet;
5. in afdeling 6.1.5. de verplichting voor de organisatie op te nemen om te garanderen dat de verwerkers met wie de gegevens zijn gedeeld of aan wie ze zijn overgedragen, de gegevens wissen, in overeenstemming met artikel 28, lid 3, punt g), AVG;
6. in afdeling 6.1.5 de zinsnede te schrappen dat de bewaartermijn onbeperkt kan zijn "(*the retention period [...] may be indefinite*").

Met betrekking tot de "algemene verplichtingen voor verwerkingsverantwoordelijken en verwerkers" adviseert de EDPB de Nederlandse toezichthoudende autoriteit om:

1. in afdeling 6.2.a "*where possible*" (indien mogelijk) te schrappen;
2. te bepalen aan welke vereisten de afspraken moeten voldoen die worden gemaakt tussen de aanvrager en de andere gezamenlijke verwerkingsverantwoordelijken die betrokken zijn bij het ToE inzake hun respectieve verantwoordelijkheden voor naleving van de Brand Compliance-certificeringscriteria;
3. in afdeling 6.4.1.b criteria op te nemen ter uitvoering van de bepalingen van artikel 26, lid 3, AVG;
4. in afdeling 7.2.b te verduidelijken dat de procedure moet waarborgen dat risicoanalyses, plannen voor de aanpak van risico's en restrisico's expliciet worden goedgekeurd door relevante directieleden;
5. in afdeling 8.7 bepalingen op te nemen over hoe er specifiek voor kan worden gezorgd dat de aanvrager aantoont met betrekking tot gegevensdoorgiften aan de AVG te voldoen.

Met betrekking tot de "rechten van betrokkenen" adviseert de EDPB de Nederlandse toezichthoudende autoriteit om:

1. in afdeling 8.2.2 een verwijzing op te nemen naar het feit dat de verwerkingsverantwoordelijke, als het verstrekken van informatie onmogelijk is of een onevenredige inspanning zou vereisen, passende maatregelen moet nemen om de rechten en vrijheden en de legitieme belangen van de betrokken te beschermen, onder meer door de informatie openbaar te maken;
2. in afdeling 8.2.2 duidelijk onderscheid te maken tussen de vrijstellingen van de informatieplicht uit hoofde van artikel 13, lid 4, AVG en uit hoofde van artikel 14, lid 5, punt b), AVG;
3. afdeling 8.2.2.b zo te wijzigen dat duidelijk is dat het op grond van de AVG niet vereist is dat een betrokkene akkoord gaat met de informatie die wordt verstrekt in overeenstemming met artikel 13 of artikel 14 AVG;
4. in afdeling 8.4.1.d de zinsnede "*for a short period of time*" (gedurende een korte periode) te schrappen;
5. in afdeling 8.4.1.e de zinsnede "[…] *within one month of receipt of the request*" (binnen een maand na ontvangst van het verzoek), die ook wordt gebruikt in artikel 12, lid 3, AVG, toe te passen;

6. in afdeling 8.4.2.b te bepalen dat de organisatie een kopie moet verschaffen van de persoonsgegevens die worden verwerkt ("[…] *provide a copy of the personal data undergoing processing*"), overeenkomstig de bepalingen in artikel 15, lid 3, AVG;
7. in afdeling 8.4.6. de bewoording "[…] *to another controller without hindrance*" (aan een andere verwerkingsverantwoordelijke, zonder daarbij te worden gehinderd) uit artikel 20, lid 1, AVG, te gebruiken om te verduidelijken dat met "*another controller*" (een andere verwerkingsverantwoordelijke) wordt verwezen naar degene die is aangemerkt door de betrokkene, en aan te geven dat het recht op overdraagbaarheid van gegevens ook van toepassing is op gegevens die zijn gegenereerd door de activiteiten van de betrokkene waar te nemen;
8. in afdeling 8.4.7 de bewoording "[…] *scientific or historical research purposes or statistical purposes*" (wetenschappelijk of historisch onderzoek of statistische doeleinden) uit artikel 21, lid 6, AVG te gebruiken;
9. de titel van afdeling 8.4.8 te veranderen in "*the right regarding automated individual decision-making, including profiling*" (het recht met betrekking tot geautomatiseerde individuele besluitvorming, waaronder profilering), in overeenstemming met de titel van artikel 22 AVG;
10. in afdeling 8.4.8 het woord "*carefully*" (nauwkeurig) te schrappen;
11. in afdeling 8.4.10 duidelijk te maken dat in beide in artikel 12, lid 5, punten a) en b), AVG genoemde scenario's moet worden aangetoond dat het verzoek kennelijk ongegrond of buitensporig is;
12. in afdeling 8.4.11 te verduidelijk of met "*complaints procedure*" (klachtenprocedure) wordt verwezen naar processen voor geschillenbeslechting of naar formele klachten uit hoofde van artikel 77, lid 1, AVG.

Met betrekking tot de "risico's voor de rechten van vrijheden van natuurlijke personen" adviseert de EDPB de Nederlandse toezichthoudende autoriteit om:

1. in afdeling 7.3a te verwijzen naar de lijsten uit hoofde van artikel 35, leden 4 en 5, AVG, zoals gepubliceerd door de Nederlandse toezichthoudende autoriteit;
2. de laatste zin van afdeling 7.3.2 te schrappen.

Tot slot wijst de EDPB er overeenkomstig zijn richtsnoeren ook op dat de Nederlandse toezichthoudende autoriteit in het geval van wijzigingen in de Brand Compliance-certificeringscriteria die substantiële veranderingen inhouden[7], de gewijzigde versie overeenkomstig artikel 42, lid 5, en artikel 43, lid 2, punt b), van de AVG bij de EDPB moet indienen.

4 SLOTOPMERKINGEN

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

Overeenkomstig artikel 64, leden 7 en 8, AVG dient de Nederlandse toezichthoudende autoriteit naar aanleiding van dit advies de voorzitter van de EDPB binnen twee weken na ontvangst van het advies langs elektronische weg mee te delen of zij haar ontwerpbesluit wijzigt dan wel handhaaft. Binnen

[7] Zie afdeling 9 van het addendum bij Richtsnoeren nr. 1/2018 voor certificering en het vaststellen van certificeringscriteria overeenkomstig de artikelen 42 en 43 van de verordening en het addendum hierbij met "Richtsnoeren voor de beoordeling van certificeringscriteria", waarvoor de periode van openbare raadpleging op 26 mei 2021 afliep.

dezelfde termijn dient zij het gewijzigde ontwerpbesluit te verstrekken of, indien zij niet van plan is het advies van de EDPB op te volgen, de redenen op te geven waarom zij voornemens is het advies geheel of gedeeltelijk niet op te volgen.

Krachtens artikel 70, lid 1, punt y), AVG zal de Nederlandse toezichthoudende autoriteit het definitieve besluit meedelen aan de EDPB zodat het kan worden opgenomen in het register van besluiten over in het kader van het coherentiemechanisme behandelde aangelegenheden.

De EDPB wijst erop dat de Nederlandse toezichthoudende autoriteit de certificeringscriteria op grond van artikel 43, lid 6, AVG openbaar moet maken in een eenvoudig toegankelijk formaat en deze moet indienen bij de EDPB voor opname in het openbare register van certificeringsmechanismen en gegevensbeschermingszegels, overeenkomstig artikel 42, lid 8, AVG.

Voor het Europees Comité voor gegevensbescherming
De voorzitter

(Anu Talus)