Opinion 26/2024 on the draft decision of the DE Bremen Supervisory Authority regarding the "Catalogue of Criteria for the Certification of IT-supported processing of Personal Data pursuant to art 42 GDPR ('GDPR – information privacy standard')" presented by datenschutz cert GmbH

Adopted on 2 December 2024

Table of contents

The European Data Protection Board

Having regard to Article 63, Article 64(1)(c) and Article 42 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the European Economic Area (hereinafter "EEA") Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Article 64(1)(c) of the GDPR and Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) Member States, supervisory authorities, the European Data Protection Board (hereinafter "the EDPB") and the European Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms (hereinafter "certification mechanisms") and of data protection seals and marks, for the purpose of demonstrating compliance with the GDPR of processing operations by controllers and processors, taking into account the specific needs of micro, small and medium-sized enterprises[2]. In addition, the establishment of certifications can enhance transparency and allow data subjects to assess the level of data protection of relevant products and services[3].
(2) The certification criteria form an integral part of any certification mechanism. Consequently, the GDPR requires the approval of national certification criteria of a certification mechanism by the competent supervisory authority (Articles 42(5) and 43(2)(b) of the GDPR), or in the case of a European Data Protection Seal, by the EDPB (Articles 42(5) and 70(1)(o) of the GDPR).
(3) When a supervisory authority (hereinafter "SA") intends to approve a certification pursuant to Article 42(5) of the GDPR, the main role of the EDPB is to ensure the consistent application of the GDPR, through the consistency mechanism referred to in Articles 63, 64 and 65 of the GDPR. In this framework, according to Article 64(1)(c) of the GDPR, the EDPB is required to issue an Opinion on the SA's draft decision approving the certification criteria.
(4) This Opinion aims to ensure the consistent application of the GDPR, including by the SAs, controllers and processors in the light of the core elements which certification mechanisms have to develop. In particular, the EDPB assessment is carried out on the basis "Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation" (hereinafter the "Guidelines") and their Addendum providing "Guidance on certification criteria assessment" (hereinafter the "Addendum").
(5) Accordingly, the EDPB acknowledges that each certification mechanism should be addressed individually and is without prejudice to the assessment of any other certification mechanism.

[1] References to "Member States" made throughout this Opinion should be understood as references to "EEA Member States".
[2] Article 42(1) of the GDPR.
[3] Recital 100 of the GDPR.

(6) Certification mechanisms should enable controllers and processors to demonstrate compliance with the GDPR; therefore, the certification criteria should properly reflect the requirements and principles concerning the protection of personal data laid down in the GDPR and contribute to its consistent application.
(7) At the same time, the certification criteria should take into account and, where appropriate, be inter-operable with other standards, such as ISO standards, and certification practices.
(8) As a result, certifications should add value to an organisation by helping to implement standardized and specified organisational and technical measures that demonstrably facilitate and enhance processing operation compliance, taking account of sector-specific requirements.
(9) The EDPB welcomes the efforts made by scheme owners to elaborate certification mechanisms, which are practical and potentially cost-effective tools to ensure greater consistency with the GDPR and foster the right to privacy and data protection of data subjects by increasing transparency.
(10) The EDPB recalls that certifications are voluntary accountability tools, and that the adherence to a certification mechanism does not reduce the responsibility of controllers or processors for compliance with the GDPR or prevent SAs from exercising their tasks and powers pursuant to the GDPR and the relevant national laws.
(11) The Opinion of the EDPB shall be adopted, pursuant to Article 64(1)(c) of GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks from the first working day after the Chair and the competent SA have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.
(12) The EDBP Opinion focusses on the certification criteria. In case the EDPB requires high level information on the evaluation methods in order to be able to thoroughly assess the auditability of the draft certification criteria in the context of its Opinion thereof, the latter does not encompass any kind of approval of such evaluation methods.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with Article 42(5) of the GDPR and the Guidelines, the "Catalogue of Criteria for the the Certification of IT-supported Processing of Personal Data pursuant to Art. 42 GDPR ('GDPR – information privacy standard')", (hereinafter the "draft certification criteria" or "certification criteria") was drafted by the datenschutz cert GmbH (hereinafter the "Datenschutz cert"), a legal entity in Germany and submitted to the Landesbeauftragte für Datenschutz Bremen, the competent German supervisory authority in Bremen (hereinafter the "DE SA (Bremen)").

2. The DE SA (Bremen) has submitted its draft decision approving the Datenschutz cert certification criteria, the draft criteria of a national certification scheme to the EDPB and requested an Opinion of the EDPB pursuant to Article 64(1)(c) GDPR on 9 October 2024. The decision on the completeness of the file was taken on 12 November 2024.

3. The present certification is not a certification according to article 46(2)(f) of the GDPR meant for international transfers of personal data and therefore does not provide appropriate safeguards within the framework of transfers of personal data to third countries or international organisations under the terms referred to in letter (f) of Article 46(2). Indeed, any transfer of personal data to a third country or to an international organisation, shall take place only if the provisions of Chapter V of the GDPR are respected.

2 ASSESSMENT

4. The Board has conducted its assessment in line with the structure foreseen in Annex 2 to the Guidelines (hereinafter "Annex") and its Addendum. Where this Opinion remains silent on a specific section of the draft certification criteria, it should be read as the Board not having any comments and not asking the DE SA (Bremen) SA to take further action.

2.1 GENERAL REMARKS

5. In the opinion of the Board, the national scope of the certification scheme is not made sufficiently clear. Notwithstanding the fact that the present opinion is directed at the DE SA (Bremen) as a prerequisite to the DE SA's administrative act of approval, which can only have a national scope, the scheme refers to member state law in several instances, which may give the impression that the scheme has a European scope in line with Article 42 (5) second sentence GDPR. Therefore, the Board recommends the competent SA to require the scheme owner to make the national scope of the certification scheme clear in the introductory text of the document. In addition, the Board encourages the competent SA to require the scheme owner to replace references to "member state law" with "German data protection law".

2.2 SCOPE OF THE CERTIFICATION MECHANISM AND TARGET OF EVALUATION (TOE)

6. The scheme is applicable for controllers and processors and for all processing operations that are IT-supported. The scheme does not include criteria for joint controllership, as a consequence, processing operations under joint controllership can not be certified under the scheme. The EDPB recommends the competent SA to require the scheme owner to clarify in the scope section that processing operations subject to joint controllership are excluded.

7. In Section 4.7.1 the catalogue contains criteria for data transfers to third countries. The EDPB notes that these criteria are included in the catalogue in order to ensure that a certified processing operation complies with the GDPR also in cases where it entails data transfers to third countries. However, the EDPB recommends the competent SA to require the scheme owner to clarify in the scope section of the scheme that the certification is not a tool for transfer according to Article 46(2) (f) GDPR.

2.3 LAWFULNESS OF PROCESSING

2.3.1 LEGAL BASIS – CONSENT

8. Regarding consent (4.1.4 P.1.4), the scheme states that consent can only be used as a legal basis if nothing prevents the termination of the processing if a potential withdrawal of consent is exercised. The EDPB encourages the competent SA to require the scheme owner to include the exceptions of Article 17 (3) GDPR into this paragraph in order to allow consent-based data processing in cases where the GDPR does not require immediate erasure in case of withdrawal. In this context the EDPB encourages the competent SA to require the scheme owner to rephrase the sentence to avoid double negations or double if-clauses and enhance clarity.

9. Regarding the consent of children, the EDPB encourages the competent SA to require the scheme owner to include a reference to the EDPB Binding Decision 2/2023 regarding TikTok in the criteria.

2.3.2 PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

10. Regarding the processing of special categories of personal data, Section 4.1.8. P.1.8 foresees the same requirements for controllers and processors and clarifies in a note that the obligation of the processor is to have processes in place to support the client (as controller) regarding his duties. The EDPB recommends the competent SA to require the scheme owner to specify in examples what would be the specific obligations of processors with regard to the different requirements listed in this section and to include a reference to the criteria from section 4.4.1, P.4.1 (Contract for commissioned personal data processing). At minimum, the processor shall be aware of the categories of data that are being processed.

2.4 PRINCIPLES OF ACRTICLE 5

2.4.1 PURPOSE LIMITATION

11. In chapter 4.2.3 (P 2.3) the scheme defines the requirements for the principle of purpose limitation. Article 6(4) GDPR is referenced, and the requirement prohibits processing operations for purposes that are incompatible with the purposes for which the data were initially collected. The provisions for the compatibility test pursuant to Article 6(4) GDPR are not fully included. The EDPB recommends the competent SA to require the scheme owner to include the detailed requirements for the compatibility test in the scheme.

12. The EDPB remarks that there is a minor mistake in the criteria in the first paragraph in this section, which starts with “The client (as controller) shall ensure that the processes (PRC) or the applications (APPL) and all other relevant assets (PO, IT, INFRA, EXT) processing personal only permit […]”. The EDPB encourages the competent SA to require the scheme owner to insert the word “data” between “personal” and “only”.

2.4.2 ACCURACY

13. In chapter 4.2.5 (P 2.5) the scheme defines the requirements for the principle of accuracy pursuant to Article 5(1)(d) GDPR. The EDPB recommends the competent SA to require the scheme owner to include in the criteria specific elements that can be used to determine and verify accuracy in data processing, as provided e.g. by the Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, chapter 3.6.

2.4.3 FAIRNESS

14. In chapter 4.2.7 (P.2.7) the scheme defines the requirements for the principle of fairness. The EDPB recommends the competent SA to require the scheme owner to include in the criteria specific elements that can be used to check the fairness of a data processing, as provided e.g. by the Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, chapter 3.3.

2.5 GENERAL OBLIGATIONS FOR CONTROLLERS AND PROCESSORS

15. The scheme is applicable for controllers and processors. The GDPR requirements for data processing differ according to the role that an entity has with regard to the processing. Consequently, the scheme makes differentiations between the certification client as controller or as processor, in order have criteria adjusted for each role. However, these detailed clarifications are usually made within a continuous text, which carries the risk that they might be overlooked. To contravene this risk, each criterion has a separate paragraph titled “Applicability according to SOA”, which specifies in general whether a criterion is applicable to controller, processor or both. The EDPB notes that the scheme includes the processor´s obligations to support and assist the controller in the fulfilment of the GDPR and therefore contains a high number of criteria that are marked as applicable for both controllers and processors and only an analysis of the criterion text will show whether the processor´s obligations with regard to this criterion equal those of the controller or are of a more supportive nature. The EDPB encourages the competent SA to require the scheme owner to enable a quicker insight into the obligations of a certification client depending on its role as controller or processor, e.g. by adding a reference sheet or matrix to the scheme or a descriptor to the section “applicability according to SOA” of each criterion which specifies whether the client is obliged to fully comply or to comply in an assisting role.

16. In section 4.6.2. P.6.2, inter alia, the appointment of the Data Protection Officer (DPO) is addressed. With regard to the necessary qualifications of a DPO, it is only generally stated that the appointment shall be based on the DPO's 'qualifications and expertise in data protection matters […]' In this regard, the EDPB recommends the competent SA to require the scheme owner to adjust the wording to align with the requirements of Article 37 (5) GDPR, which states that the DPO shall be designated 'on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices […]'.

17. In section 4.6.2. P.6.2, the term 'data privacy officer' is used at least once. The EDPB recommends the competent SA to require the scheme owner to use the term 'data protection officer' consistently instead, in line with the GDPR definition.

18. Furthermore, in section 4.6.2. P.6.2, it is stipulated that the DPO 'shall report directly to the highest management level of the client (as controller or processor) and shall not receive

instructions.' In accordance with Article 38 (3) GDPR, the EDPB recommends the competent SA to require the scheme owner to clarify the wording to specify that the DPO '[…] shall not receive any instructions regarding the exercise of his tasks' (meaning the tasks referred to in Article 39 GDPR).

19. The EDPB notes that in section 4.6.4. P.6.4, it is stipulated that 'The processor's, or where applicable, the controller's representative, Record of processing activities (ROPA) shall contain at least the following information […]'. Since this relates to requirements for processors, this sentence should be modified to refer to the 'processor's representative'. Therefore, the EDPB recommends the competent SA to require the scheme owner to change it accordingly.

2.5.1 Processing operations (PO) and Processes (PRC) as asset categories and processes as (additional) requirements in the criteria

20. In the introduction, the scheme introduces the different asset categories that are a part of the target of evaluation. In addition to the Processing Operations (PO), in which personal data are being processed, the scheme defines processes (PRC) as activities that use inputs to deliver an intended result required for the data processing. Several criteria refer explicitly to these processes as (additional) requirements to fulfil the criteria, in many cases, the criteria for controllers are rounded up by the requirement for a process that needs to be in place to ensure the continuous fulfilment of the criterion. With regard to processors, the scheme repeatedly requires them to have processes in place to assist the controller in the fulfilment of legal obligations that apply for controllers. As a result, the criteria contain a mix of legal or technical obligations and processes required to assure that these obligations are continuously fulfilled and/or processes that the processor needs to have in place in order to assist the controller. The EDPB notes that these different requirements are not always listed in the same sequence and encourages the competent SA to require the scheme owner to facilitate orientation in the scheme by implementing a more consistent sequence, that would ideally start with the legal or technical requirement for the controller, complemented by the requirement for the processes that are necessary to ensure continuous fulfilment and rounded up by the requirements for the processor.

2.5.2 Obligations applicable to processors

21. In section 4.4.1 P.4.1, the scheme defines the criteria for the contract according to art. 28 GDPR, differentiating between the controller to processor contract and the processor to subprocessor contract. The following section (4.4.2 P.4.2) deals with the implementation of the measures under the controller to processor contract. The section lacks requirements for measures under the processor to subprocessor contract. While these measures may be similar to the measures under the controller to processor contract, the EDPB still recommends the competent SA to require the scheme owner to make the measures explicit.

2.6 RIGHTS OF DATA SUBJECTS

22. In section 4.8, the data subject rights according to Chapter III of the GDPR are addressed. The EDPB notes that this section does not discuss the possible exceptions under Article 23 GDPR, which allows for certain restrictions of these rights under specific conditions. In light of this, the EDPB recommends the competent SA to require the scheme owner to establish criteria

that check whether restrictions of data subject rights set out in German Member State law apply to and are in line with the processing operations within the Target of Evaluation.

23. Furthermore, the EDPB notes that the modalities for data subject rights under Article 12 GDPR are repeated for each data subject right in the respective chapter of section 4.8. While this does not lead to incomplete criteria, it can affect the flow of reading and overall clarity. Therefore, the EDPB encourages the competent SA to require the scheme owner to address the modalities under Article 12 GDPR fully once at the beginning of section 4.8, rather than repeating them for each data subject right.

24. Insofar as section 4.8 addresses criteria for processors in relation to data subject rights, the EDPB notes that these provisions are of general nature only. According to the criteria, 'the client (as processor) shall implement processes (PRC) to assist the controller in fulfilling this obligation […]'. However, there are no specific provisions detailing how this assistance obligation is to be implemented in relation to each individual data subject right, which raises concerns about the auditability of these criteria. Therefore, the EDPB recommends the competent SA to require the scheme owner to include more specific criteria for the assistance obligations of processors for each data subject right.

25. In the context of the right of access under Section 4.8.1 P.8.1, reference is made inter alia to 'the origin of the data' as part of the information to be provided. The EDPB recommends the competent SA to require the scheme owner to align the wording with Article 15 (1) (g) GDPR, which states that '[…] any available information as to their source' shall be provided.

26. In Section 4.8.1 P.8.1, reference is also made to Article 12 (5) GDPR. However, there are no criteria for assessing when requests from a data subject are considered 'manifestly unfounded or excessive.' The EDPB therefore recommends the competent SA to require the scheme owner to include criteria for such an assessment. The EDPB “Guidelines 01/2022 on data subject rights - Right of access” (6.3.2) provides a number of possible criteria in this regard.

27. In section 4.8.7 P.8.7 the scheme defines the criteria for the Right to object under Article 21 GDPR. While all relevant aspects are included, the criterion does not follow the structure of Article 21 which can lead to confusion. The EDPB recommends the competent SA to require the scheme owner to restructure the section following the structure of Article 21.

28. In section 4.8.8. P.8.8, the 'revocation of consent' is addressed. Among other things, the requirement is that the withdrawal of consent shall lead to the termination of the data processing unless there are alternative legal grounds. To avoid any ambiguities, the EDPB recommends the competent SA to require the scheme owner to include a reference to Article 17 (1) (b) GDPR in this context.

29. In section 4.3.1 P.3.1, the scheme defines the criteria regarding the information of the data subject. The requirements of articles 13 and 14 GDPR are contained in the same chapter. The EDPB encourages the competent SA to require the scheme owner to separate these criteria into different chapters to facilitate the overview and improve readability and improve auditability.

30. With regard to the information obligations in case of data not collected form the data subjects (art. 14) the requirements point out the exceptions to the information obligation laid down in article 14 (5). The EDPB encourages the competent SA to require the scheme owner to add

criteria to check the proportionality of the effort involved and to define the possibility/impossibility of informing the data subject.

2.7 RISKS FOR THE RIGHTS AND FREEDOMS OF NATURAL PERSONS AND TECHNICAL AND ORGANISATIONAL MEASURES GUARANTEEING PROTECTION

31. Regarding the implementation of technical and organisational measures (TOMs) by a processor in section 4.5.1, P.5.1, there is no reference to the instructions by the controller and in particular, Article 28 (3) (c) GDPR. However, the Board notes that the implementation of risk-based TOMs by a processor is, in addition, affected by the "controller to processor contract". In light of this, the EDPB recommends the competent SA to require the scheme owner to include a reference to the criteria from section 4.4.1, P.4.1 (Contract for commissioned personal data processing) in the aforementioned section 4.5.1, P.5.1.

32. In section 4.5.1. P.5.1, the determination of appropriate technical and organisational measures is addressed. According to this section, the first step is an analysis of the data processing as a whole, including all assets. This section provides general conditions for conducting such analysis but does not include more information on methodology. Therefore, the EDPB encourages the competent SA to require the scheme owner to clarify that the applicant is required to apply recognized risk assessment methods.

33. In Section 4.5.5. P.5.5, the term 'organization' is used in the first bullet point, which apparently refers to the client (the controller or processor to be certified). To avoid misunderstandings and to ensure consistent terminology, the EDPB encourages the competent SA to require the scheme owner to use the term 'client' instead of 'organization' in this context.

34. Furthermore, section 4.6.5 P.6.5 addresses the requirements for when a data protection impact assessment (DPIA) shall be carried out. While reference is made to the lists pursuant to Article 35 (4) and (5) GDPR, these are not specified. The EDPB therefore recommends the competent SA to require the scheme owner to clarify that only lists of the competent (German) SA for controller or processor need to be taken into account.

2.8 CRITERIA FOR THE PURPOSE OF DEMONSTRATING THE EXISTENCE OF APPROPRIATE SAFEGUARDS FOR TRANSFER OF PERSONAL DATA

35. In the context of data transfers to third countries under section 4.7.1 P.7.1, the EDPB points out that, in line with the EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, the first step in assessing the admissibility of such transfers is always the recording and mapping of all such data transfers ('Know your transfers'). The EDPB therefore recommends the competent SA to require the scheme owner to explicitly include this requirement. If this requirement is already addressed elsewhere in the present criteria, the EDPB recommends the competent SA to require the scheme owner to include a cross-reference in section 4.7.1 P.7.1.

36. Furthermore, the EDPB notes that according to section 4.7.1. P.7.1, it shall be ensured that data transfers to third countries are 'permitted'. To provide more clarity, the EDPB encourages

the competent SA to require the scheme owner to specify that data transfers to third countries 'shall always be carried out in accordance with the provisions of Chapter V of the GDPR.'

37. As general remark to this section the EDPB notes that the section covers several Articles. While all relevant aspects are included, the section lacks a clear structure. The EDPB therefore encourages the competent SA to require the scheme owner to restructure the section or add headlines in between the different transfer tools.

3 CONCLUSIONS / RECOMMENDATIONS

By way of conclusion, the EDPB considers that:

38. regarding the "scope of the certification mechanism and target of evaluation (ToE)", the Board recommends that the DE SA (Bremen) requires the scheme owner to:

    1. make the national scope of the certification scheme clear in the introductory text of the document;
    2. clarify in the scope section that processing operations subject to joint controllership are excluded;
    3. clarify in the scope section of the scheme that the certification is not a tool for transfer according to art 46(2) (f) GDPR;

39. regarding the "lawfulness of the processing" the Board recommends that the DE SA (Bremen) requires the scheme owner to:

    1. specify in examples what would be the specific obligations of processors with regard to the different requirements listed in this section and to include a reference to the criteria from section 4.4.1, P.4.1 (Contract for commissioned personal data processing);

40. regarding the "principles of Article 5 GDPR" the Board recommends that the DE SA (Bremen) requires the scheme owner to:

    1. include the detailed requirements for the compatibility test pursuant to Article 6 (4) GDPR in the scheme;
    2. include in the criteria specific elements that can be used to determine and verify accuracy in data processing, as provided e.g. by the Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, chapter 3.6;
    3. include in the criteria specific elements that can be used to check the fairness of a data processing, as provided e.g. by the Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, chapter 3.3;

41. regarding the "general obligations for controllers and processors" the Board recommends that the DE SA (Bremen) requires the scheme owner to:

    1. adjust the wording to align with the requirements of Article 37 (5) GDPR, which states that the DPO shall be designated "on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices […]";

2. use the term “data protection officer” consistently, in line with the GDPR definition;

3. clarify the wording to specify that the DPO “[…] shall not receive any instructions regarding the exercise of his tasks” (meaning the tasks referred to in Article 39 GDPR);

4. change the sentence “The processor's, or where applicable, the controller's representative, Record of processing activities (ROPA) shall contain at least the following information […]” to refer to the “processor's representative”;

5. make the measures under the processor to subprocessor contract explicit;

42. regarding the “rights of data subjects” the Board recommends that the DE SA (Bremen) requires the scheme owner to:

    1. establish criteria that check whether restrictions of data subject rights set out in German Member State law apply to and are in line with the processing operations within the Target of Evaluation.

    2. include more specific criteria for the assistance obligations of processors for each data subject right;

    3. align the wording regarding the “origin of the data” with Article 15 (1) (g) GDPR, which states that “[…] any available information as to their source” shall be provided;

    4. include criteria for an assessment of “manifestly unfounded or excessive' requests”;

    5. restructure the section on the Right to Object following the structure of Article 21 GDPR;

    6. include a reference to Article 17 (1) (b) GDPR in the context of revocation of consent;

43. regarding the “risks for the rights and freedoms of natural persons” and the “technical and organisational measures guaranteeing protection” the Board recommends that the DE SA (Bremen) requires the scheme owner to:

    1. include a reference to the criteria from section 4.4.1, P.4.1 (Contract for commissioned personal data processing) in section 4.5.1, P.5.1. (implementation of technical and organisational measures (TOM) by a processor);

    2. clarify that only lists pursuant to Article 35 (4) and (5) GDPR, of the competent (German) SA for controller or processor need to be taken into account;

44. regarding “criteria for the purpose of demonstrating the existence of appropriate safeguards for transfer of personal data” the Board recommends that the DE SA (Bremen) requires the scheme owner to:

    1. include a requirement for a first step in assessing the admissibility of such transfers, which is the recording and mapping of all data transfers (“Know your transfers"). If this requirement is already addressed elsewhere in the present criteria, the EDPB recommends the competent SA to require the scheme owner to include a cross-reference in section 4.7.1 P.7.1.

45. Finally, in line with the Guidelines the EDPB also recalls that, in case of amendments of the “Catalogue of Criteria for the Certification of IT-supported Processing of Personal Data

pursuant to Art. 42 GDPR ('GDPR – information privacy standard')" involving substantial changes[4], the DE SA (Bremen) will have to submit the modified version to the EDPB in accordance with Articles 42(5) and 43(2)(b) of the GDPR.

4 FINAL REMARKS

46. This Opinion is addressed to the DE SA (Bremen) and will be made public pursuant to Article 64(5)(b) of the GDPR.

47. According to Article 64(7) and (8) of the GDPR, the DE SA (Bremen) shall communicate its response to this Opinion to the Chair by electronic means within two weeks after receiving the Opinion, whether it will amend or maintain its draft decision. Within the same period, it shall provide the amended draft decision or where it does not intend to follow the Opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this Opinion, in whole or in part.

48. Pursuant to Article 70(1)(y) GDPR, the DE SA (Bremen) shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

49. The EDPB recalls that, pursuant to Article 43(6) of the GDPR, the DE SA (Bremen) shall make public the Datenschutz cert certification criteria in an easily accessible form, and transmit them to the Board for inclusion in the public register of certification mechanisms and data protection seals, as per Article 42(8) of the GDPR.

For the European Data Protection Board

The Chair
Anu Talus

[4] See section 9 of the Addendum to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation providing "Guidance on certification criteria assessment".