Opinion 18/2024 on the draft decision of the Austrian Supervisory Authority regarding DSGVO-zt GmbH certification criteria

Adopted on 16 July 2024

Table of contents

1 SUMMARY OF THE FACTS 4
2 ASSESSMENT 5
2.1 GENERAL REMARKS 5
2.2 SCOPE OF THE CERTIFICATION MECHANISM AND TARGET OF EVALUATION (TOE) 6
2.3 CERTIFICATION CRITERIA 7
2.4 LAWFULNESS OF PROCESSING 7
2.5 PRINCIPLES OF ARTICLE 5 7
2.6 GENERAL OBLIGATIONS FOR CONTROLLERS AND PROCESSORS 8
2.7 RIGHTS OF DATA SUBJECTS 9
2.8 TECHNICAL AND ORGANISATIONAL MEASURES GUARANTEEING PROTECTION 9
2.9 CRITERIA FOR THE PURPOSE OF DEMONSTRATING THE EXISTENCE OF APPROPRIATE SAFEGUARDS FOR TRANSFER OF PERSONAL DATA 10
3 CONCLUSIONS / RECOMMENDATIONS 10
4 FINAL REMARKS 12

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) 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) GDPR), or in the case of a European Data Protection Seal, by the EDPB (Articles 42(5) and 70(1)(o) GDPR).
(3) When a supervisory authority (hereinafter "SA") intends to approve a certification pursuant to Article 42(5) 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 GDPR. In this framework, according to Article 64(1)(c) 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"), for which the public consultation period expired on 26 May 2021.

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

(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.
(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) 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) GDPR and the Guidelines, the “DSGVO-zt GmbH Certification criteria” (hereinafter the “draft certification criteria” or “certification criteria”) were drafted by DSGVO-zt GmbH, a legal entity in Austria, and submitted to the Datenschutzbehörde, the Austrian Supervisory Authority (hereinafter the “AT SA”).

2. The AT SA has submitted its draft decision approving the certification criteria, and requested an Opinion of the EDPB pursuant to Article 64(1)(c) GDPR on 11 April 2024.The decision on the completeness of the file was taken on 29 May 2024.

2 ASSESSMENT

3. 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 AT SA to take further action.

4. These certification criteria are national criteria pursuant to Article 42(5) GDPR and are not intended to be an EU Data Protection Seal.

5. The present certification is not a certification according to article 46(2)(f) 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 GDPR are respected.

2.1 GENERAL REMARKS

6. With respect to section 2.4 of the draft certification requirements, the Board notes that they refer to GDPR certification, pursuant to Article 42(1) GDPR, intended to enable a controller or a processor to demonstrate that the certified processing of personal data is carried out in strict compliance with the GDPR. However, the Board understands that this certification criteria are relevant only for controllers and not for processors. Therefore, the Board recommends the AT SA to require the scheme owner to modify this section accordingly for clarity purposes.

7. Moreover, the Board notices that the draft certification criteria, in section 4 on "normative references", refer to the "test scope" of the present certification criteria. The Board is not familiar with the "test scope" concept, thus recommends the AT SA to require the scheme owner to clarify in the criteria what this term means.

8. Furthermore, in the same section, the Board notes that the reference to the national accreditation requirements is missing and thus recommends the AT SA to require the scheme owner to modify this section of the criteria accordingly.

9. The Board notes that throughout the draft certification criteria there are references to the content of GDPR provisions. In the same context, the Board notes that some references to the relevant GDPR articles are missing. For example in section 2.7 of the draft certification criteria, there is a reference to Recital 100 GDPR, which is not entirely in line with the wording of the relevant GDPR Recital. Similarly, in section 5.2.5 and 5.2.20 of the draft certification criteria on the definitions of data subject and PIA - which the Board understands that refers to the DPIA concept of the GDPR - the definitions are not fully aligned with the ones of the GDPR. For consistency purposes, the Board recommends the AT SA to require the scheme owner, where GDPR definitions are used, to ensure that they are used consistently, as well as to ensure that the appropriate references to the GDPR provisions are made.

10. The Board notes that in some criteria it is not entirely clear what needs to be audited. The Board underlines that this should be made clear from the criteria themselves. In this regard, the Board notes that the draft certification criteria do not always define the elements upon which the assessment should be carried out so to make clear what is expected to be

demonstrated by the applicant and audited by the certification body. For example, in section 2.11 of the draft certification criteria there is a reference to "appropriate measures" which must "effectively" impact the respective level of protection. In this context, the Board notices that the factors to be taken into account for identifying the measures as "appropriate" and their "effective" impact are missing from the draft certification criteria, which can jeopardise the conduct of the audit by the certification body. Similarly, in section 2.12, the draft certification criteria refer to "adequate" measures. Finally, the relevant factors to be taken into account, are not established by the criteria. Taking all the above into account, the Board recommends the AT SA to require the scheme owner to modify these certification criteria, by further elaborating on the factors to be taken into account when the relevant assessments are carried out.

11. With respect to section 3 of the draft certification criteria on "scope of application", the Board understands that this refers to the Target of Evaluation, thus recommends the AT SA to require the scheme owner to modify the title of this section by renaming it accordingly for clarity purposes.

12. With respect to section 5.1 of the draft certification criteria, the Board encourages the AT SA to require the scheme owner to further specify that, where available, GDPR definitions prevail. Similarly, throughout Section 5 of the draft certification criteria, the Board encourages the AT SA to require the scheme owner to add a reference to "EDPB relevant Guidelines" and "applicable case law", considering that these two sources shall be taken into account by controllers in their compliance efforts, given the fact they further specify GDPR concepts and definitions.

13. With respect to Section 2.11.3 of the Attachment to annex I, the Board encourages the AT SA to require the scheme owner to clarify that "the intended transport route shall be determined and documented"**.**

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

14. The Board welcomes the explanations provided within section 2.3 of the draft certification criteria about the fact that the criteria are not a mechanism that demonstrates the existence of appropriate safeguards under Article 42(2) and Article 46(2)(f) GPDR for the international transfers of personal data. For completeness purposes, the Board encourages the AT SA to require the scheme owner to add this element also in section 3 on the "scope of application".

15. With respect to section 3.1 of the draft certification criteria on the "scope of application" the Board recommends deleting the reference to "certifying a product or a service" as only processing operations can be certified according to the GDPR.

16. Regarding section 3.2 of the draft certification criteria, the Board encourages the AT SA to require the scheme owner to add that the description of the Target of Evaluation shall not only be "detailed", but also "complete".

17. In the same section of the draft certification criteria (i.e. 3.2) the Board notes that the criteria refer to a list of "partners". For the Board is not entirely clear what the term "partners" entails, thus it encourages the AT SA to require the scheme owner to clarify this in the criteria.

18. Similarly, the Board notices that the criteria in this section do not refer to "processors", but only to "sub-processors". Therefore, it encourages the AT SA to require the scheme owner to add "processors" as well.

2.3 CERTIFICATION CRITERIA

19. The Board understands the complementary nature of the Annex I (technical and organisational measures) to the core certification criteria, based on section 8 of the draft certification criteria, that "In the event that certain measures of Annex I are not implemented because they are not applicable to the specific data processing context or because the implementation of these measures would have no effect on residual data processing risks, the applicant shall provide the certification body with adequate and detailed documentation to substantiate these decisions. The non-implementation of security measures shall not be based on the applicant's decision to accept a higher residual risk. On request of the certification body, the applicant must provide a list of measures of Annex I that have not been implemented". The Board takes note of this, but recommends the AT SA to require the scheme owner to clarify in which cases the non-applicability of the measures included in Annex I will take place and provide more information on how this non-applicability will be justified by the applicant. As an example, in section 2.8.15 of the attachment to the Annex I regarding "email encryption", it should be further clarified i) under which circumstances and; ii) what kind of justification would be enough to be provided by the applicant in order to deviate from applying this measure.

2.4 LAWFULNESS OF PROCESSING

20. The Board notes that in section 7.1.2.2.b of the draft certification criteria, the latter mention that "Where the request for consent is made by an information society service to a minor who, under the provisions of the Member State, can validly give such consent only with the consent of the holder of parental responsibility, the procedure shall include obtaining consent or assent from the holder of pa-rental responsibility". The Board understands that the reference to the provisions of the Member States relate to the applicable provisions under national law. Therefore, the Board encourages the AT SA to require the scheme owner to modify this criterion accordingly.

2.5 PRINCIPLES OF ARTICLE 5

21. The Board notes that in the draft certification criteria, section 6 which refers to accountability includes criteria related to a) data processing impact assessment, b) involvement of processors, c) records of processing activities and d) personal data breaches. The Board highlights in this regards, that the principle of accountability, pursuant to Article 5(2) GDPR is an overarching principle which horizontally applies to all the obligations of controllers. Thus the Board for clarity and consistency purposes recommends the AT SA to require the scheme owner to clarify in the certification criteria that the accountability principle covers all the criteria and not only the ones mentioned under section 6 (e.g. by changing the name of this section).

22. The Board welcomes the inclusion of the fairness principle in section 7.2 of the draft certification criteria together with the reference to the EDPB Guidelines 2/2019 on the processing of personal data under art 6(1)(b) GDPR in the context of the provision of online services to data subjects. However, the Board would like to highlight that the certification

criteria shall be a "stand-alone" document, where all the criteria are sufficiently and specifically elaborated so to achieve having auditable criteria. In this regard, the Board notes that within its Guidelines 04/2019 on Article 25 GDPR Data Protection by Design and by Default, the Board lists several elements that need to be taken into account in order to comply with the principle of fairness. Therefore, for completeness and auditability of the criteria, the Board recommends the AT SA to require the scheme owner to further develop specific, precise and auditable criteria, in cases that they are not already covered in other parts of the criteria, based on all the elements listed in the EDPB Guidelines 4/2019 on Article 25 GDPR regarding Data Protection by Design and by Default, adopted on 20 October 2020, paragraph 70.

2.6 GENERAL OBLIGATIONS FOR CONTROLLERS AND PROCESSORS

23. When defining the ToE, the Board recommends to define the requirements to be met regarding the arrangement concluded between the applicant and potential joint-controllers involved in the ToE with regards to their respective responsibilities for compliance with the certification criteria.

24. Moreover, the Board recommends to include criteria that implement the provisions of Article 26(3) GDPR.

25. The Board notes that section 6.2.3 of the draft certification criteria is not consistent with the wording of Article 28(2) GDPR which states that "The processor shall not engage another processor without prior specific or general written authorisation of the controller [...]". In particular, the Board recommends the AT SA to require the scheme owner to adapt section 6.2.3 by reversing the order of the words "written" and "general" in order to not give the misleading impression that only the "general authorisation" needs to be in writing.

26. The Board notes that section 6.1.1(d) of the draft certification criteria does not refer to Article 35(4) GDPR and recommends the AT SA to require the scheme owner to include a reference to this provision and to the list of the type of processing operations which are subject to the requirement for a data protection impact assessment pursuant to Article 35(1) GDPR.

27. With regards to section 6.1.6 of the draft certification criteria on "continuous evaluation", the Board notes that the criteria (in footnote 9), with regards to a "recognised assessment methodology", refer to two documents issued by the European Union Agency for Cybersecurity (ENISA). The Board encourages the AT SA to require the scheme owner to clarify that these documents are merely an example of recognised assessment methodologies and to further specify in the criteria that the latest version of relevant standards shall be taken into account in this context.

28. Along the same lines, the Board encourages the AT SA to require the scheme owner to further explain what the ENISA documents refer to and avoid using links in the criteria, to ensure the access to the relevant documents in the future.

29. The Board notes that in section 6.3 the draft certification criteria refer to **"**The purpose of the records of processing activities pursuant to Art. 30 GDPR is to provide an overview of the processing activities and the associated risks to the rights and freedoms of data subjects as well as the remedial measures taken". The Board highlights that the associated risks and the remedial measures are additional to the information that the records of processing shall contain pursuant to Article 30 GDPR. Therefore, the Board encourages the AT SA to require the scheme owner to either modify this requirement so not to give the impression that the

GDPR requires to include the risks and remedial measures in the record of processing or to explain in the criteria that the inclusion of this information in the records of processing is not mandatory pursuant to Article 30 GDPR.

2.7 RIGHTS OF DATA SUBJECTS

The Board notes that in section 6.4.1(d) the draft certification criteria refer to "Recognized method for assessing whether there is likely to be a risk or a high risk". The Board recommends to add the link between the high risk and the fundamental rights and freedoms of the data subjects so as to align this criterion with the wording of the GDPR.

2.8 TECHNICAL AND ORGANISATIONAL MEASURES GUARANTEEING PROTECTION

30. The Board notes the core certification criteria are complemented with two documents, namely "Annex I" which outlines the main technical and organisation measures, and "Attachement to Annex I" which further specifies them. The Board understands that these two documents are fully part of the criteria and that it is mandatory to check all the criteria, while it is only possible to exclude certain technical and organizational measures by providing the certification body with a documented justification that they are not relevant to the processing activity in question. The Board also understands that the certification body will always conduct an assessment of the non-applicability of some criteria.

31. Furthermore, in Attachment to Annex I, paragraphs 2.2.1, 2.2.2, and 2.2.3, the Board notes that some terms cannot be assessed objectively (e.g. "especially", "to easily monitored", "if all employ-ees know each other"). The Board recommends the AT SA to require the scheme owner to delete these references in order to avoid ambiguity of the criteria.

32. Similarly, in Attachment to Annex I, paragraph 2.2.8, the Boards considers that stating that "The risk of recovery must be minimised depending on the respective protection requirements by adhering to common norms and standards" is not sufficiently precise. Therefore, the Board recommends the AT SA to require the scheme owner to further specify and include more specific guidance (e.g. by defining norms or standards to be used as model, and by referring to "the state of the art").

33. The Board notes that in the attachment to Annex I, section 2.8.15, there is reference to email encryption: "E-mails containing personal data must be protected against unauthorised access. Depending on the respective content, transport encryption or end-to-end encryption must be used for this purpose. As a rule of thumb, transport encryption is to be implemented regardless of content, for special categories of data end-to-end encryption should be mandatory at least in the course of planned business processes". The Board encourages the AT SA to require the scheme owner to either delete this exemption, as it is not only relevant for email encryption, or in order to avoid misunderstandings, to relocate this under another part of the criteria (i.e. in Annex I, section 3).

34. Furthermore, the Board encourages the AT SA to require the scheme owner to clarify and highlight the exceptional character of this measure and to also make a reference to Article 9(2)(c) GDPR.

35. In section 6.2.1 of the draft certification criteria, there is a reference to "Procedures to ensure that only processors that provide sufficient guarantees, in particular in terms of expertise, reliability and resources, that appropriate technical and organisational measures are

implemented in such a way that the processing complies with these certification criteria are used". The Board notes that the technical and organisational measures for the controller are listed in line with the criteria of section 8 of the certification criteria. Therefore, for the better readability and accuracy of section 6.2.1, the Board encourages the AT SA to require the scheme owner to refer to the section 8 of the draft certification criteria.

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

36. The Board could not identify specific criteria related to Article 48 GDPR ("Transfers or disclosures not authorised by Union law"). In this regards, the Board recommends the AT SA to require the scheme owner to add a criterion to the effect that a third country's request to transfer or disclose personal data does not, as such, make a transfer or disclosure lawful under Article 48 GDPR.

3 CONCLUSIONS / RECOMMENDATIONS

By way of conclusion, the EDPB considers that:

37. regarding the "general remarks", the Board recommends that the AT SA requires the scheme owner to:

    1. modify section 2.4 in order to clarify that the certification criteria are relevant only for controllers and not for processors;
    2. clarify in section 4 of the certification criteria the term "test scope";
    3. add in section 4 of the certification criteria the missing reference to accreditation requirements;
    4. ensure, throughout the certification criteria, that where GDPR definitions are used, they are used consistently and that the appropriate references to GDPR provisions are made;
    5. modify sections 2.11 and 2.12 of the certification criteria, by further elaborating on the factors to be taken into account when the relevant assessments are carried out;
    6. modify section 3 of the certification criteria on "scope application" by renaming it, for clarity purposes;

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

    1. delete, in section 3.1 of the certification criteria, the reference to "certifying a product or a service" as only processing operations ca be certified according to the GDPR;

39. regarding the "certification criteria" the Board recommends that the AT SA requires the scheme owner to:

    1. clarify in which cases the non-applicability of the measures included in Annex I will take place and provide more information on how this non-applicability will be justified by the applicant. As an example, in section 2.8.15 of the attachment to the Annex I regarding "email encryption", it should be further clarified i) under which circumstances and; ii) what kind of justification would be enough to be provided by the applicant in order to deviate from applying this measure;

40. regarding the “principles of Article 5” the Board recommends that the AT SA requires the scheme owner to:

    1. clarify in the certification criteria that the accountability principle of Article 5(2) GDPR covers all the criteria and not only the ones mentioned under section 6 of the certification criteria (i.e. a) data processing impact assessment, b) involvement of processors, c) records of processing activities and d) personal data breaches;
    2. in section 7.2 of the certification criteria, develop specific, precise and auditable criteria, in cases that they are not already covered in other parts of the criteria, based on all the elements listed in the EDPB Guidelines 4/2019 on Article 25 GDPR regarding Data Protection by Design and by Default;

41. regarding the “general obligations for controllers and processors” the Board recommends that AT SA requires the scheme owner to:

    1. when defining ToE, to define the requirements to be met regarding the arrangement concluded between the applicant and potential joint-controllers, involved in the ToE with regards to their respective responsibilities for compliance with the certification criteria;
    2. include criteria that implement provisions of Article 26(3) GDPR;
    3. adapt section 6.2.3 of the certification criteria, by reversing the order of the words “written” and “general” in order not to give the misleading impression that only the “general authorisation” needs to be in writing;
    4. include a reference to Article 35(4) GDPR and to the list of the type of the processing operations which are subject to the requirement for a data protection impact assessment pursuant to Article 35(1) GDPR;

42. regarding the “rights of data subjects” the Board recommends that AT SA requires the scheme owner to:

    1. add, in section 6.4.1(d) the link between the high risk and the fundamental rights and freedoms of the data subjects so to align this criterion with the GDPR wording;

43. regarding the “technical and organisation measures guaranteeing protection” the Board recommends that AT SA requires the scheme owner to:

    1. in the attachment to Annex I, paragraphs 2.2.1, 2.2.2, and 2.2.3, delete some terms that cannot be assessed objectively (e.g. “especially”, “to easily monitored”, “if all employ-ees know each other”), in order to avoid ambiguity in the criteria;
    2. further specify and include more specific guidance in paragraph 2.2.8 of the Attachment to Annex I (e.g. by defining norms or standards to be used as model, and by referring to the “state of the art”);

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

    1. add a criterion, to the effect that a third country’s request to transfer or disclose personal data does not, as such, make a transfer or disclosure lawful under Article 48 GDPR;

45. Finally, in line with the Guidelines the EDPB also recalls that, in case of amendments of the DSGVO-zt GmbH certification criteria involving substantial changes[4], the AT SA 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 AT SA and will be made public pursuant to Article 64(5)(b) GDPR.

47. According to Article 64(7) and (8) GDPR, the AT SA 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 AT SA 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) GDPR, the AT SA shall make public the DSGVO-zt GmbH 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) 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" for which the public consultation period expired on 26 May 2021.