
# Opinion 15/2025 on the draft decision of the Austrian Supervisory Authority (AT SA) regarding the certification criteria of BDO Consulting GmbH

**Adopted on 8 July 2025**

# 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 "CERTIFICATION CRITERIA FOR CERTIFICATION PROCEDURES IN ACCORDANCE WITH ARTICLE 42 GDPR" (hereinafter the "draft certification criteria" or "certification criteria") were drafted by BDO Consulting GmbH, a legal entity registered in Austria (217731v) and submitted to 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 29 April 2025. The decision on the completeness of the file was taken on 17 June 2025.

3. The present certification criteria have a general scope and are not limited to specific processing operations. Certification of processing operations carried out by controllers and processors is possible.

4. Certification of joint controllers under Article 26 GDPR is excluded from the scope of the certification criteria. Furthermore, certification is not available for companies that do not have an establishment within the EEA.

5. 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

6. 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 certification criteria, it should be read as the Board not having any comments and not asking the AT SA to take further action.

## 2.1 GENERAL REMARKS

7. The Board notes that, in section 1.1 on "target of evaluation", the draft certification criteria provide that "The target of evaluation can encompass processes, processing operations and systems. The Board highlights that only processing operations can be certified, thus recommends the AT SA to require the scheme owner to delete the reference to "systems" for accuracy purposes.

8. With respect to section 2.2 on "Structure of the certification criteria" of the draft certification criteria, the Board encourages the AT SA to require the scheme owner to add a specific reference to "EDPB relevant Guidelines", "relevant guidelines or recommendations of the Article 29 Working Party" and "applicable case law" under the sub-section "Additional Guidance", considering that these three sources shall be taken into account by controllers and/or processors in their compliance efforts, given the fact they further specify GDPR concepts and definitions, and further specify that, where available, GDPR definitions prevail.

9. Similarly, the Board notes that during its first plenary meeting it endorsed the GDPR related WP29 Guidelines[4]. Therefore, the Board encourages the AT SA to require the scheme owner to explicitly state whether the WP29 Guidelines referred to in the draft certification criteria are endorsed by the EDPB.

10. Furthermore, the Board encourages the AT SA to require the scheme owner to delete the word "former" from the references to the Article 29 Working Party.

11. In addition, the Board notices that the draft certification criteria A.01.02 (for controllers) on Data protection organisation including roles and responsibilities" and B.01.01 (for processors) on "Data protection organisation including roles and responsibilities" refer

[4] The WP29 Guidelines which were endorsed by the EDPB are listed here: https://www.edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en.

to the term “Data Protection Coordinators”. The Board welcomes the use of this term. However, to enhance the readability and understanding of the certification criteria the Board recommends that the above-mentioned term be clearly defined. To this purpose, the Board recommends the AT SA to require the scheme owner to either define the term “Data Protection Coordinators” under the section on “general definitions” or clearly define this term within the criteria themselves.

12. With regards some of the draft certification criteria, the Board notes that there is a need for further alignment with the GDPR. This applies in particular to the criteria listed below:

- Draft certification criterion A.02.03 - measures for implementing the principle of data minimization: The criterion reads as follows: The certification applicant shall ensure compliance with the principle of data minimization as per Article 5 GDPR. The certification applicant shall ensure that the personal data processed are limited to what is necessary for the purposes of the processing”. However, Article 5(1)(c) GDPR reads as follows: “Personal data shall be: adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’)”. Therefore, the fact that the personal data processed are “adequate, relevant and limited to what is necessary” is missing.
- Draft certification criterion A.02.04 - Measures for implementing the principle of accuracy: The criterion requires that the certification applicant shall establish a process for maintaining personal data accurate that consider the following for the processing activities intended for certification: [...] Measures for checking processed data for accuracy and currency, as well as for correcting them. However, Article 5(1)(d) GDPR also states that: “every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay”. Therefore, the element of “erasing the data without undue delay” is missing.
- Draft certification criterion A.02.10 - Legal basis for the processing of special categories of personal data: The provision under the GDPR reads as follows: “processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim”. However, the reference to the potential philosophical aim of the foundation, association or any other not-for-profit body is missing from the detailed requirement.
- Draft certification criterion A.02.10 - Legal basis for the processing of special categories of personal data: The provision of Article 9(2)(b) GDPR reads as follows: “a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject”. However, the reference to the list of safeguards (technical and organizational measures - TOMs) to protect the fundamental rights and interests of the data subjects and that these safeguards shall be kept up to date and risk-appropriate through an appropriate process (cf. criterion A.06.01) is missing from the detailed requirement.
- Draft certification criterion A.02.10 - Legal basis for the processing of special categories of personal data: The provision of Article 9(2)(f) GDPR reads as follows: “processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity”. However, the reference “or

whenever courts are acting in their judicial capacity" is missing from the detailed requirement.

- Draft certification criterion A.03.01 - Process for handling data subject requests: According to the GDPR "the controller shall provide information on action taken on a request under Articles 15-22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary". These deadlines are missing from the criteria.
- Draft certification criterion A.03.01 - Process for handling data subject requests: The process for handling data subject requests shall also include a point on determining cases where a reasonable fee might be charged taking into account the administrative costs of providing the information or communication or taking the action requested pursuant to Article 12(5) GDPR. This element is not included in the criteria.
- Draft certification criterion A.03.04 - Right of access by the data subject: Point 4 of this criterion reads as follows: "The certification applicant shall document the time of the data (copy) provided, including details of the information request". Article 15(3) GDPR reads as follows: "Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form". This element is not included in the criteria.
- Draft certification criterion A.03.11 - Restrictions on data subjects' rights under Union or national law: Based on Article 23(1) GDPR "Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard: ...". However, the detailed requirement of this criterion quotes only Articles 12 to 22 GDPR. A relevant reference to Articles 34, , as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, in line with Article 23(1) GDPR, are missing from this criterion. Furthermore, the detailed requirement of the same criterion does not quote that the essence of fundamental rights and freedoms is set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.
- Draft certification criterion A.10.01 - Appointment of a data protection officer: The last sentence of the detailed requirement of this criterion reads as follows: "If the certification applicant has formally appointed a data protection officer, the contact details of the data protection officer shall be demonstrably brought to the attention of the individuals within the organization and the contact details of the data protection officer shall be demonstrably communicated to the supervisory authority". However, Article 37(7) GDPR also requires the publication of the contact details of the DPO. This element is missing from the criteria.
- Draft certification criterion A.10.02 - Job or task description of the data protection officer: The second bullet point under the detailed requirement reads as follows: "Monitoring compliance with the GDPR and the controller's or processor's personal data protection policies, including the assignment of responsibilities, awareness-raising and training of staff involved in the processing operations and the related

audits;". However, the same task under Article 39(1)(b) GDPR reads as follows: "to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits. The reference to the Austrian data protection law is missing.

- Draft certification criterion A.04.07 - Verification of the security of data processing: Under the detailed requirement of this criterion, it is stated that "In assessing whether the processor complies with the contractual obligations, in particular to implement and maintain adequate technical and organizational measures, the certification applicant may also use compliance with approved codes of conduct under Article 40 or a certification procedure under Article 42 GDPR". The reference to Article 28(5) GDPR, which is the relevant GDPR provision, is missing in the "references" part.
- Draft certification criterion A.08.03 - Notification of a personal data breach to the supervisory authority: While the detailed requirement of this criterion includes the wording of the provision under Article 33(4) GDPR, Article 33(4) GDPR is missing from the references of this criterion.
- Draft certification criterion A.09.01 - Assessment and documentation of a Data Protection Impact Assessment (DPIA): Article 35(1) GDPR requires that the context of the processing shall also be taken into account by the certification applicant when determining whether a DPIA is necessary. However, this criterion refers only to the nature, scope and purposes of the processing.
- Draft certification criterion B.08.01 - Notification of personal data breaches to the controller: While the detailed requirement of this criterion includes the wording of the provision under Article 33(4) GDPR, Article 33(4) GDPR is missing from the references of this criterion.
- Draft certification criterion B.10.01 - Appointment of a data protection officer: The last sentence of the detailed requirement of this criterion reads as follows: "If the certification applicant has formally appointed a data protection officer, the contact details of the data protection officer shall be demonstrably brought to the attention of the individuals within the organization and the contact details of the data protection officer shall be demonstrably communicated to the supervisory authority". However, Article 37(7) GDPR also requires the publication of the contact details of the DPO. This element is missing from the criteria.
- Draft certification criterion B.10.02 - Job or task description of the data protection officer: The second bullet point under the detailed requirement reads as follows: "Monitoring compliance with the GDPR and the controller's or processor's personal data protection policies, including the assignment of responsibilities, awareness-raising and training of staff involved in the processing operations and the related audits;". However, the same task under Article 39(1)(b) GDPR reads as follows: "to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits. The reference to the Austrian data protection law is missing.

Therefore, regarding all the above, the Board recommends the AT SA to require the scheme owner to amend the above-mentioned criteria so to bring them in line with the GDPR.

13. Furthermore, the Board notices that the draft certification criteria B.04.04 ("Processing of personal data only on the basis of a documented instruction from the controller") and B.04.08 ("Requirements for compliance with the obligations defined in the data processing agreement") refer to the term "customer". To enhance the readability and understanding of the certification criteria the Board recommends the AT SA to require the scheme owner to replace the above-mentioned term with the term "controller" for consistency and accuracy purposes.

## 2.2 Scope of the Certification mechanism and Target of Evaluation (ToE)

14. With respect to section 3 on "Non-applicability of certification criteria" of the draft certification criteria, the Board acknowledges that some criteria may not be relevant depending on the data processing circumstances. However, the Board notes that the terms "For example" and "may" can lead to ambiguity and can hinder the auditability of the criteria. To this purpose, the Board recommends the AT SA to require the scheme owner to include the conditions to be met in order to establish the non-applicability of a criterion as an integral part of the criteria by default, delete the term "For example" and replace the term "may" with the term "shall".

## 2.3 Lawfulness of Processing

15. The Board takes note of draft certification criterion A.02.09 on "declaration of consent of a child in information society services" and that fact that the criterion provides that "the certification applicant shall establish a process for all processing activities within the scope of certification: The measures taken to verify the age of the child and to obtain the consent of the holder of parental responsibility over the child, including verification of entitlement to custody (for example, uploading a copy of a passport and birth certificate can be taken as a prerequisite for accepting an application to enter into an insurance contract)". The Board, based on the AT SA's explanations understands that request for the birth certificate will not be applicable under all circumstances, thus encourages the AT SA to require the scheme owner to modify this criterion in order to avoid misunderstanding.

16. With respect to the draft certification criterion A.02.10 on the "legal basis for the processing of special categories of personal data", the Board takes note of the fact that the option c refers, in line with the Article 9(2)(c) of the GDPR, to the vital interests of data subject or another natural person (Article 9(2)(c) GDPR). However, the sub-point b makes an explicit reference to the protection of the **life** of the data subject as a vital interest. Since the protection of the life is not the only situation that vital interest is triggered, whilst Article 9(2)(c) GDPR also refers to possible vital interests of another natural person, the Board recommends AT SA to require the scheme owner to amend the sub-point b, so as to clarify that documentation is needed why the processing is necessary to protect vital interests (e.g., the life) of the data subject or of another natural person and why it cannot be based on any other legal basis.

## 2.4 Legal Basis

### 2.4.1 Legal Basis - Consent

17. The Board takes note that there are two different draft certification criteria on consent (i.e. 02.07.01 on "consent for the processing of personal data" and A.02.08 on "form of declaration of consent"). The Board is of the opinion that these two criteria overlap and that the criterion A.02.08 itself is not clear enough. Therefore, the Board encourages the AT SA to require the scheme owner to modify these criteria and merge them so to avoid confusion.

18. Similarly, the Board recommends the AT SA to require the scheme owner to include Article 7 GDPR in the references of this criterion for sake of completeness.

19. Furthermore, the draft certification criterion A.02.10 on the "Legal basis for the processing of special categories of personal data" requires that the required documentation shall include a list of safeguards (technical and organizational measures - TOMs) to protect the fundamental rights and interests of the data subjects and that these safeguards shall be kept up to date and risk-appropriate through an appropriate process. The Board understands that the "appropriate safeguards" provided in Article 9(2) GDPR are interpreted in the criteria as being limited only to technical and organisational measures. Therefore, the Board recommends the AT SA to require the scheme owner to add the wording "in particular" in order to clarify that these safeguards are not exhaustive and that other safeguards could also be included.

### 2.4.2 Legal Basis - Processing of personal data for the performance of a task carried out in the public interest or in the exercise of official authority

20. In the draft certification criterion A.02.07.05 on "Processing of personal data for the performance of a task carried out in the public interest or in the exercise of official authority", the scheme defines the requirements for this legal basis. The Board encourages the AT SA to require the scheme owner to modify the title of this criterion and add "vested in the certification applicant as controller" in line with the description of this criterion and the provision of Article 6(1)(e) GDPR.

## 2.5 Principles of Article 5

21. In the draft certification criterion A.01.01 on "Compliance with Article 5 GDPR (Accountability) by implementing a data protection policy", the scheme defines the topics, which shall be encompassed by the data protection policy, including further references to the specific criteria which are relevant to each topic. More specifically, with respect to the topic on "Data protection organisation and responsibilities (see draft certification criterion A.01.02)", the general reference to the draft certification criterion A.01.02 can lead to ambiguity and can hinder the auditability of the criteria. Therefore, the Board encourages the AT SA to require the scheme owner to further specify that the data protection policy shall contain the identity and the contact details of the controller, the contact details of the data protection officer (if applicable), the contact details of the data protection coordinators (if applicable),the legal basis of the processing operation

or operations, the recipients or categories of recipients of the personal data and whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.

22. Regarding the accountability, the Board notes that the draft certification criterion A.01.01 on "Compliance with Article 5 GDPR (Accountability) by implementing a data protection policy" states that "The certification applicant shall be able to guarantee and demonstrate compliance with the principles for processing personal data set out in Article 5 GDPR. Therefore, the certification applicant shall ensure that policies are defined". The Board notes that according to Article 5(2) GDPR[5] the controller shall not only be able but also shall be responsible for demonstrating compliance with Article 5(1) GDPR. Therefore, the Board recommends that the AT SA requires the scheme owner to modify this criterion to align its wording with the wording of the provision of Article 5(2) GDPR.

23. The Board welcomes the fact that the draft certification criterion A.02.01 on "Measures for implementing the principle of transparency" only refers to Article 5(1)(a) GDPR and recital 39 GDPR as well as the fact that the detailed requirement of the same criterion refers to Articles 13-14, 15-22 and 34 GDPR. However, the Board notes that the principle of transparency is embedded also in Article 12[6]. Therefore, the Board recommends the AT SA to require the scheme owner to include the reference to Article 12 GDPR under the detailed requirement that the certification applicant shall have rules, a mechanism or a procedure in place to ensure transparency requirements in the GDPR meaning that information is provided to data subjects (under Articles 13-14 GDPR) for completeness and consistency purposes.

24. Furthermore, the Board welcomes the fact that the draft certification criterion A.02.01 on "Measures for implementing the principle of transparency" requires that the information or communication with data subjects shall comply with the use of a clear and plain language. However, the Board notes that the use of a clear and plain language shall be ensured when providing information to every data subject and not be limited only in cases of providing information to children. Therefore, the Board recommends the AT SA to require the scheme owner to delete the wording "(when providing information to children)" from the detailed requirements of the criterion for accuracy purposes.

25. The Board also welcomes the section on "Application Guidance" of the draft certification criterion A.02.01 on "Measures for implementing the principle of transparency" and in particular the reference to the "Guidelines on Transparency under Regulation 2016/679 (WP 260 rev.01)" of the former Article 29 Working Party. However, the Board notes that the EDPB succeeded the Article 29 Working party set up under Article 29 of Directive 95/46/EC, which was repealed on 25 May 2018, when the GDPR entered into

[5] Article 5(2) GDPR reads as follows: "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')".
[6] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020, paragraph 65, available here: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

application, and adopted the Guidelines 4/2019 on Article 25 Data Protection by Design and by Default[7], which shall be taken into account by controllers and/or processors in their compliance efforts. Therefore, the Board recommends the AT SA to require the scheme owner to add a reference to the "EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, adopted on 20 October 2020".

26. The Board notes that while for the principle of transparency there are detailed criteria, for the fairness principle this is not the case. In this context, the Board reiterates that the certification criteria shall be a stand-alone document, where all the criteria are sufficiently and specifically elaborated to be auditable. In this regard, the Board notes that within its Guidelines 04/2019 on Article 25 GDPR Data Protection by Design and by Default (adopted on 20 October 2020), the Board lists several elements that should 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 so far 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, paragraph 70 (see also EDPB Opinion 3/2025).

27. The Board welcomes the draft certification criterion A.02.02 on "Measures for implementing the principle of purpose limitation" and in particular the requirement that the certification applicant shall establish and maintain documentation for all processing activities intended for certification, comprising of description of the purposes of each processing activity to be certified and privacy statement that provides information on the purposes of the processing activities to be certified for which the personal data are intended. However, the Board notes that while for the principles of accuracy, integrity and confidentiality the certification applicant shall also document measures taken to implement these principles, for the purpose limitation principle this is not the case. Therefore, for the sake of completeness, the Board encourages the AT SA to require the scheme owner to specify that the certification applicant shall implement measures: (i) before considering carrying out any personal data processing, to determine the purposes of the processing; (ii) if a change in processing is envisaged, to determine whether this change concerns the purposes of the processing; and (iii) to prevent misuse of purposes, and document these measures.

28. In the draft certification criterion A.02.02 on "Measures for implementing the principle of purpose limitation", the scheme defines the requirements for the principle of purpose limitation and criterion A.02.07.07 prohibits further processing of personal data for purposes that are incompatible with the specified, explicit and legitimate purposes for which the data were initially collected. However, the Board notes that the scheme does not mention the exclusion of processing activities falling under Articles 85 to 89 GDPR and a reference to such processing is included under criterion A.02.10. Therefore, the Board understands that relevant aspects of GDPR compliance with regard to the processing operations falling under those Articles are meant to be covered by the certification criteria. Consequently, the Board recommends to clarify that further

[7] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020, available here: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en

processing for archiving in the public interest, scientific or historical research, or statistical purposes is not per se considered contrary to the original purpose (singular), provided that an assessment of the purpose compatibility is duly documented especially with regard to the existence of appropriate safeguards for the rights and freedoms of the data subject. In particular, the Board is of the opinion that the appropriate safeguards for the rights and freedoms of data subjects in place for each processing operation carried out for archiving purposes in the public interest, for scientific or historical research or for statistical purposes should also be documented by the organisation and assessed as part of the compatibility test referred to in criterion A.02.07.07.

## 2.6. General Obligations for Controllers and Processors

### *2.6.1. Obligation applicable to controllers and processor*

29. With respect to the draft certification criteria A.01.03 (for controllers) and B.01.02 (for processors) on "Regular training and awareness - raising measures for employees", the Board notes that the certification applicant shall inform employees about the data protection requirements only of the GDPR, whereas EU data protection legislation is comprised of the General Data Protection Directive (GDPR) and the Austrian Data Protection Act. Therefore, for the sake of completeness and accuracy of these criteria, the Board encourages the AT SA to require the scheme owner to also replace the wording "General Data Protection Regulation" with "data protection laws".

30. Moreover, the draft certification criteria A.10.03 (for controllers) and B.10.03 (for processors) require that the applicant provide evidence of, *inter alia*, the measure that adequate temporal, organizational, and financial resources are provided for the proper fulfillment of all DPO tasks, and the allocation of these resources is documented. However, Article 38(2) GDPR states that: "The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge", meaning that it refers to the more general term "resources", which also includes time, training and equipment. For that reason, the EDPB recommends the AT SA to require the scheme owner to adapt the criteria, to the effect that the resources allocated to the DPO do not only cover performance of tasks, but also maintenance of knowledge, in line with Article 38(2) GDPR.

### *2.6.2. Obligations applicable to the controllers*

31. With respect to section A.01.03 of the draft certification criteria on "Regular training and awareness - raising measures for employees" the Board welcomes the criteria thereof. However, the Board notes that, while the draft certification criteria include criteria in detail for processors, the areas in which the training measures shall raise awareness do not include the relationship with processors. Therefore, the Board encourages the AT SA to require the scheme owner to modify this criterion accordingly and include a presentation on relationships with processors in the areas in which the training measures shall raise awareness for employees.

*2.6.3 Obligations applicable to processors*

32. With respect to the draft certification criterion A.04.05 on "Agreements for data processing with data processors that meet all requirements of Article 28 GDPR", the Board welcomes the inclusion of the obligation of the data processor to ensure that another processor is only engaged with prior specific or general written authorisation of the controller. The Board also notes that the criterion A.04.06 on the "Right to object to further sub-processors" requires the certification applicant to ensure that the contracted data processors do not engage further sub-processors unless there is written consent from the data controller, in line with Article 28(2) GDPR. The Board encourages the AT SA to require the scheme owner to include a reference to criterion A.04.06 under criterion A.04.05 for the sake of completeness.

33. With respect to the draft certification criterion B.07.09 on "Procedure for data pseudonymization or anonymization", the Board welcomes the criteria thereof. However, the Board notes that the similar draft certification criterion A.07.09 for controllers requires that the documentation of the measures used for pseudo- and anonymization shall also present where feasible, a demonstration/justification of the effectiveness of the procedure. Therefore, the Board encourages the AT SA to require the scheme owner to modify this criterion accordingly for consistency purposes.

34. Draft certification criterion B.08.01 on "notification of personal data breaches to controller" provide that the processor shall inform the controller about the data breach without undue delay and where possible within 72 hours. The Board is of the opinion that the obligation to notify the controller within 72 hours lowers the standards of the GDPR, which provides that the processor should notify the controller without undue delay. Therefore, the Board recommends the AT SA to require the scheme owner to modify this criterion by removing the timeline of 72 hours.

## 2.7 Rights of data subjects

35. The Board welcomes the fact that in section 4.8 of the draft certification criteria on the "rights of data subjects", the criteria refer to the fact that the certification applicant has to implement a process for handling the data subjects' requests (Articles 12-22 GDPR) and responding "without undue delay, and in any event, within a month". However, the Board notes that for the right of access, under section A.03.04 of the certification criteria, the reference to the timing to respond to data subject's request is missing. Therefore, the Board recommends the AT SA to require the scheme owner to modify this criterion accordingly and include the reference to timing for completeness and consistency purposes.

36. The Board also welcomes the fact that in the same section of the draft certification criteria, the criteria include the requirement to verify the identity of the data subject and document the steps taken to verify the identity of the data subject where the certification applicant has reasonable doubts concerning the identity of the natural person making the request. However, the Board recommends the AT SA to require the scheme owner to also specify the means by which the proof of identity may be provided by the data subject.

## 2.8 Technical and organisational measures guaranteeing protection

37. With respect to the draft certification criterion A.04.01 on “data protection by design” the Board welcomes the criteria thereof. However, the Board notes that the draft criteria do not mention that it is required by Article 25 GDPR to decide at very early stage how the data protection principles shall apply. For completeness and accuracy purposes, the Board recommends that the AT SA requires the scheme owner to bring this criterion in line with the GDPR.

38. Similarly, the Board notes that the reference to the very early stage of the processing is missing also in the relevant criteria on “support in the implementation of data protection by design” under the draft certification criterion B.04.01.1. Therefore, the Board recommends the AT SA to require the scheme owner to also modify this draft criterion accordingly.

39. Regarding draft criterion A.01.04, “Ongoing monitoring of compliance with data protection requirements”, the Board welcomes the inclusion of the statement that “the certification applicant shall have a monitoring plan, that covers all data protection activities to be monitored in a risk-oriented manner over a defined period of time according to a "risk map" of the company or organization”. However, taking into account that the term “monitoring plan” can lead to ambiguity and can hinder the auditability of this criterion, the Board recommends the AT SA to require the scheme owner to modify this criterion, to also require that the applicant shall set up a monitoring procedure allowing all data protection activities to be analysed.

40. With respect to the draft certification criterion A.06.03 (for controllers) on “regular review of the risk analysis” the criteria mention that “the risk analysis which were carried out by the certification applicant shall be reviewed regularly”. In this context the Board notes that the term “regularly” can be quite broad, can lead to ambiguity and can hinder the auditability of this criterion. To this purpose, the Board recommends the AT SA to require the scheme owner to further elaborate on the regularity of audits and to adjust the relevant criteria to the effect that require applicants to implement risk management procedures for continuous adjustment of measures adopted in order to comply with this criterion.

41. Similarly, with respect to the draft certification criteria (for processors) B.06.03 on “regular review of the risk analysis”, the Board recommends the AT SA To require the scheme owner to further elaborate on the regularity of audits and to adjust the relevant criteria to the effect that require applicants to implement risk management procedures for continuous adjustment of measures adopted in order to comply with this criterion.

42. Furthermore, the Board welcomes the draft certification criterion A.07.21 (for controllers) and the draft certification criterion B.07.21 (for processors) on “Guidelines for employees on the handling of removable storage devices” and the requirement for a topic-specific policy. However, the Board notes that this topic-specific policy seems to be independent from the risk management procedure. Therefore, the Board recommends the AT SA to require the scheme owner to amend this criteria, so as to ensure that this policy shall be aligned with the overall risk management procedure.

43. The Board takes note of the draft certification criteria A.07.24 (for controllers) and B.07.24 (for processors) on the “examination of the effectiveness of technical and

organisational measures", which refer to the fact that "The certification applicant shall conduct regular checks to ensure the effectiveness of the technical and organisational measures adopted". In this context the Board notes that the term "regular" can be quite broad, can lead to ambiguity and can hinder the auditability of this criterion. Therefore, the Board recommends to further specify and elaborate what which checks qualify as "regular" checks so to promote the auditability of this criteria.

44. The Board welcomes the draft certification criteria A.07.02 (for controllers) and criteria B.07.02 (for processors), which refer to "malware protection and updates". However, the Board considers that this is not enough and that the criteria should have policies/procedures on the outcome of risk management and to not be seemed as isolated criteria on malware for both auditability and effectiveness purposes. Thus, the Board recommends the AT SA to require the scheme owner to develop such policies and insert them in the criteria.

45. In addition, the Board is of the opinion that there is a need for alignment between A.07.02 criteria and criteria A.06.01 and A.06.02 (for controllers) on document of a risk management process and on risk-oriented measures to ensure the security of data processing (risk-control matrix) respectively). What applies for criteria A.07.02 also applies to criteria A.07.03 – A.07.10, A.07.14 – A.07.18 (i.e. the current content does not seem to be sufficient. Accordingly, the relevant criteria for processors, namely criteria B.06.01 and criteria B.06.02, also seem to be insufficient. Therefore, for completeness purposes the Board recommends the AT SA to require the scheme owner to modify these criteria.

# 3 CONCLUSIONS / RECOMMENDATIONS

46. By way of conclusion, the EDPB considers that the present certification criteria may lead to an inconsistent application of the GDPR and the following changes need to be made in order to fulfil the requirements imposed by Article 42 of the GDPR in light of the Guidelines and the Addendum:

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

1. delete the reference to "systems" from section 1.1 on "target of evaluation" for accuracy purposes;

2. define the term "Data Protection Coordinators" under the section on "general definitions" or clearly define this term within the criteria themselves to enhance the readability and understanding of the criteria

3. amend the criteria listed in paragraph 12 of this Opinion so to bring them in line with the GDPR;

4. to replace the term "customer" with the term "controller" in the criteria B.04.04 ("Processing of personal data only on the basis of a documented instruction from the controller") and B.04.08 ("Requirements for compliance with the obligations defined in the data processing agreement") for consistency and accuracy purposes;

48. regarding the “scope of the certification mechanism and target evaluation (ToE)”, the Board recommends that the AT SA requires the scheme owner to:

    1. include the conditions to be met in order to establish the non-applicability of a criterion as an integral part of the criteria by default, delete the term “For example” and replace the term “may” with the term “shall”;

49. regarding the “lawfulness of processing” the Board recommends that the AT SA requires the scheme owner to:

    1. amend the sub-point b of the criterion A.02.10, so as to clarify that documentation is needed why the processing is necessary to protect vital interests (e.g., the life) of the data subject or of another natural person and why it cannot be based on any other legal basis;

50. regarding the “legal basis” the Board recommends that the AT SA requires the scheme owner to:

    1. include Article 7 GDPR in the references of the criterion on consent for sake of completeness;

    2. add the wording “in particular” in order to clarify that other safeguards could also be included in the documentation required under the criterion A.02.10;

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

    1. modify the criterion A.01.01 to align its wording with the wording of the provision of Article 5(2) GDPR;

    2. include the reference to Article 12 GDPR under the detailed requirement of the criterion A.02.01 that the certification applicant shall have rules, a mechanism or a procedure in place to ensure transparency requirements in the GDPR meaning that information is provided to data subjects (under Articles 13-14 GDPR) for completeness and consistency purposes;

    3. delete the wording “(when providing information to children)” from the detailed requirements of the criterion A.02.01 for accuracy purposes;

    4. add a reference to the “EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, adopted on 20 October 2020” in the section on “Application Guidance” of the criterion A.02.01;

    5. further develop specific, precise and auditable criteria for the fairness principle, in so far 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, paragraph 70 (see also EDPB Opinion 3/2025);

    6. clarify under the criterion A.02.07.07 that further processing for archiving in the public interest, scientific or historical research, or statistical purposes is not per se considered contrary to the original purpose (singular), provided that an assessment of the purpose compatibility is duly documented especially with regard to the existence of appropriate safeguards for the rights and freedoms of the data subject;

52. regarding the "general obligations for controllers and processors" the Board recommends that the AT SA requires the scheme owner to:

    1. adapt the criteria A.10.03 (for controllers) and B.10.03 (for processors), to the effect that the resources allocated to the DPO do not only cover performance of tasks, but also maintenance of knowledge, in line with Article 38(2) GDPR;

    2. modify the criterion B.08.01 by removing the timeline of 72 hours;

53. regarding the "rights of data subjects" the Board recommends that the AT SA requires the scheme owner to:

    1. modify the criterion A.03.04 and include the reference to timing for completeness and consistency purposes;

    2. specify the means by which the proof of identity may be provided by the data subject;

54. regarding the "technical and organisational measures guaranteeing protection" the Board recommends that the AT SA requires the scheme owner to:

    1. bring the criterion A.04.01 in line with the GDPR for completeness and accuracy purposes;

    2. modify the criterion B.04.01.1 and include a reference to the very early stage of the processing;

    3. modify the criterion A.01.04 to also require that the applicant shall set up a monitoring procedure allowing all data protection activities to be analysed;

    4. further elaborate on the regularity of audits and to adjust the criterion A.06.03 to the effect that require applicants to implement risk management procedures for continuous adjustment of measures adopted in order to comply with this criterion;

    5. further elaborate on the regularity of audits and to adjust the criterion B.06.03 to the effect that require applicants to implement risk management procedures for continuous adjustment of measures adopted in order to comply with this criterion;

    6. amend the criteria A.07.21 (for controllers) and B.07.21 (for processors), so as to ensure that this policy shall be aligned with the overall risk management procedure;

    7. further specify and elaborate what which checks qualify as "regular" checks so to promote the auditability of the criteria A.07.24 (for controllers) and B.07.24 (for processors);

    8. develop policies on the outcome of risk management and insert them in the criteria A.07.02 (for controllers) and B.07.02 (for processors);

    9. align the criterion A.07.02 with the criteria A.06.01 and A.06.02 (for controllers) and the criterion B.06.01 with the criterion B.06.02 (for processors) for completeness purposes.

55. Finally, in line with the Guidelines the EDPB also recalls that, in case of amendments of the certification criteria of BDO Consulting GmbH certification criteria involving substantial

changes[8], 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

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

57. According to Article 64(7) and (8) of the 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.

58. 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.

59. The EDPB recalls that, pursuant to Article 43(6) of the GDPR, the AT SA shall make public the GDPR-CARPA 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)

[8] 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.