Opinion 1/2022 on the draft decision of the Luxembourg Supervisory Authority regarding the GDPR – CARPA certification criteria

Adopted on 1 February 2022

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"), 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) of the GDPR.
[3] Recital 100 of the 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) 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 "GDPR-CARPA certification criteria" (hereinafter the "draft certification criteria" or "certification criteria") was drafted by the Luxemburg Supervisory Authority (hereinafter the "LU SA").

2. The LU SA has submitted its draft decision approving the GDPR-CARPA certification criteria, and requested an Opinion of the EDPB pursuant to Article 64(1)(c) GDPR on 1 October 2021. The decision on the completeness of the file was taken on 28 October 2021.

   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

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 LU SA's draft certification criteria, it should be read as the Board not having any comments and not asking the LU SA to take further action.

2.1 General remarks

4. The Board notes that the terms used throughout the document can sometimes be confusing. An example regarding the consistency of the terminology can be found under section I-13, where there is a reference to "persons concerned", which should be replaced with "data subjects". Therefore, the Board encourages the LU SA to ensure the consistency of the term used throughout the draft certification criteria.

5. The Board encourages to clarify the meaning of some of the terms used in the certification criteria, such as the entity's "authorized" management that is required to supervise the implementation of the mechanism supported by its DPO for international data transfers so as to ensure their compliance with the GDPR (see criteria II-a-18 and III-13, but also I-1) and the "formal assessment" required to be performed by the entity as it is mentioned several times throughout the draft criteria (e.g. section II-a-10).

6. The draft criteria state in several sections that "the entity has taken into account the formal opinion of its DPO" (e.g. sections II-a-18 and III-13)." The Board encourages the LU SA to clarify, in a note in the draft criteria, that the DPO, even if he/she has a significant role for the compliance monitoring of the entity's processing activities according to Article 39 of the GDPR, the latter should not be the one responsible to assess the implementation of the measures designed to ensure such compliance.

7. The Board notes that the certification criteria submitted by the LU SA do not contain any information on the planned evaluation methods. According to the LU SA, these can be derived (in part) from the International Standard on Assurance Engagements (ISAE 3000 standard), which is part of the certification process as it is used in connection with the accreditation. Based on the information provided by the SA, this standard has been developed by the International Auditing and Assurance Standards Board (IAASB) and deals with assurance engagements other than audits or reviews of historical financial information. The EDPB encourages the LU SA to clarify that the ISAE 3000 standard is not of relevance for the certification criteria as it is not part of it, but it is relevant for the certification process. In this regard the EDPB recalls what already recommended in the context of its Opinion on the accreditation requirements for LU SA's certification bodies.[4]

[4] See EDPB Opinion 5/2020 on the draft decision of the competent supervisory authority of Luxemburg regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43(3) (GDPR), adopted on 29 January, para. 8.

2.2 Scope of the certification mechanism and Target of Evaluation (ToE)

8. The GDPR-CARPA certification scheme is a general scheme in that does not focus on a specific sector or type of processing. According to the information provided by LU SA, the main object of the certification scope are the data protection responsibilities of the controller / processor (accountability principle). For this reason, the GDPR-CARPA includes requirements focusing on the data protection governance in the organization surrounding the processing activities included the TOE in addition to specific criteria concerning directly those processing activities. However, the LU SA established some scope limitations / exclusions to clarify which (type of) processing activities can / cannot be certified under GDPR-CARPA certification scheme. In particular, GDPR-CARPA is not suitable for:

- certifying personal data processing specifically targeting minors under 16 years old;
- certifying processing activities in the context of a joint controllership;
- certifying processing activities in the context of article 10 GDPR;
- entities that have not officially designated a DPO (article 37 GDPR).

In this regard, the Board notes that the GDPR CARPA scheme does not mention the exclusion of processing activities falling under Articles 85 to 89 GDPR. However, 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. For example, section II-a-9 of the draft certification criteria concerns the processing of special categories of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, but it does not mention the suitable and specific measures to safeguard the fundamental rights and interests of data subjects required under Article 89(1) of the GDPR. Therefore, the Board recommends the LU SA to include specific criteria covering processing activities under Articles 85 to 89 of the GDPR.

Furthermore, the Board recommends the LU SA to include that an analysis of the relevant laws shall be performed by the entity which demonstrates that specific and suitable measures have been put in place in order to respect the fundamental rights and interests of data subjects pursuant to Article 89 of the GDPR.

2.3 Procedure to determine a Target of Evaluation (ToE)

9. According to the information provided by the LU SA, the TOE for the certification has to be setup following the "Planning and Performing the Engagement" requirements of the International Standard on Assurance Engagements (ISAE standard), which is part of the certification process. However, as stated in the EDPB Guidelines 1/2018, how the ToE has to be defined should be sufficiently described in the certification criteria themselves (see Annex 2 to the EDPB Guidelines 1/2018, section 2.f). This seems not to be the case for the GDPR-CARPA certification scheme which in this regard relies on the ISAE standard, while provides guidance to define the TOE in the certification program. In this context, the Board recommends the LU SA to include in the beginning of the draft certification criteria, in a devoted section, sufficient information with regard to the criteria on how the ToE is defined.

2.4 Certification criteria

10. The Board notes that in a large number of the criteria it is not clear what needs to be audited and by whom. On the contrary, the Board, underlines that this should be made clear from the criteria themselves. In particular, the tool of "self-assessment" by the applicant is used in many criteria. In this regard, the Board notes that the LU SA does not always define in the criteria the elements upon which the self-assessment should be carried out by the applicant so as to make clear what is expected to be demonstrated by the applicant and audited by the certification body. For example, sections II-a-I and II-a-4 about identification of a valid legal basis and data processing based on contract respectively do not specify the factors that should be taken into account by the applicant when carrying out the assessment on the identification of the legal basis, such as the necessity of the processing in relation to the purposes pursued and the appropriateness of the legal basis considering the processing activities, depending on the nature, context, scope and purposes of the processing. The same applies to the other criteria concerning the rest of the legal grounds (i-e. II-a-3 and II-a-5-8).

    In that respect, it should be avoided that the certification body takes over the assessment of the applicant without checking or at least critically questioning it with regard to the said factors to be specified in the criteria. This applies in particular to the criteria listed below:

    - Section II-a-I and II-a-3 to II-a-8 with regard to the above-mentioned factors regarding the assessment on the identification of the legal basis of the data processing.
    - Section I-14 regarding data breaches in relation to the factors to be taken into account for the required assessment.
    - Similarly, in section I-15 regarding the notification of data breaches towards the controller, with reference to the factors to be considered in the context of the assessment of those breaches.
    - Section II-a-11 regarding the rights to restriction of the processing, with respect to the factors to be taken into account, to establish the impossibility or disproportionate character of the communication to the recipients to whom personal have been disclosed.
    - Similarly, in section II-a-14 regarding the factors to be taken into account to determine if the provision of information to data subjects in accordance with Article 14 of the GDPR proves impossible or would involve a disproportionate effort.
    - Section II-a-18 regarding third country transfers, see the specific recommendation in paragraph 22 of this Opinion.
    - Section II-b-2 regarding purpose compatibility, see the specific recommendation in paragraph 23 of this Opinion.
    - Section II-c-2 regarding alternative means, with respect to the factors be taken into account when assessing whether there is an impossibility to reach the purposes by implementing a less intrusive process (e.g. amount of data collected, retention period, aim of processing, technology available).

- Section II-d-3 regarding the right to rectification, in relation to the factors on which the assessment of impossibility or disproportionate character of the communication to the recipients to whom personal have been disclosed should be based.
- Section II-e-1 regarding the defined retention period omits to provide the factors that should be taken into account in case the retention period cannot be established in light of the applicable legal requirements (e.g. purpose(s) pursued).
- Section II-e-3 regarding the right to erasure, with reference to the factors to consider in the assessment of the impossibility or disproportionate character of the communication to the recipients to whom personal have been disclosed.
- Section II-f-2 regarding the risk analysis, see the specific recommendation in paragraph 52.
- Section II-f-9 regarding the assessment of sufficiency, see the specific encouragement in paragraph 35.
- Section III-7 regarding the risk treatment see the specific recommendation in paragraph 55.
- Section III-3 regarding the transfers to third countries, see the specific recommendation in paragraph 22.

Therefore, the Board recommends the LU SA to amend the above-mentioned criteria to provide the factors that shall be taken into account by the applicant when carrying out the relevant assessments so as to also clarify what will be checked by the certification body.

2.5 Lawfulness of Processing

11. The Board notes that under section II-a-I, the LU SA makes reference to a "valid legal basis". However, the Board is of the opinion that the LU SA should take into account how the applicability of the legal basis is demonstrated and its appropriateness, where relevant, considering the processing activities, depending on the nature, context, scope and purposes of the processing. The Board recommends the LU SA to modify this criterion accordingly.[5]

12. Under section II-a-3 it is mentioned that "the entity has analysed the necessity of consent". The Board recommends the LU SA to take into account that the entity demonstrates the appropriateness of consent as the legal ground for the processing in the individual case, instead of its necessity so to have this criterion in line with Recital 43 of the GDPR and the EDPB Guidelines on consent under the GDPR.[6]

13. Under section II-a -3, regarding "freely given" consent the Board encourages the LU SA to add a reference to Recital 32 for completeness.

[5]See Recital 43 of the GDPR as well as the EDPB Guidelines 05/2020 on consent under the GDPR available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

[6] See for instance paragraphs 2, 3, 16, 17, 31 and 91 of the EDPB Guidelines 05/2020 on consent under the GDPR available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

14. The Board takes note of the requirement of informed and unambiguous consent in section II-a-3. However, the Board considers that more information is needed thereof. More precisely, the Board recommends that the LU SA adds in its draft certification criteria the minimum requirements which have to necessarily be met so that consent can be considered informed and unambiguous and that the criteria bring sufficient added value for the compliance with the GDPR of the certified entities.

15. Under section II-a-8, the draft certification criteria state: "The legislator provides by law for the legal basis for public authorities to process personal data". Consequently, this legal basis should not apply to the processing by public authorities in the performance of their tasks". In this regard, the EDPB encourages the LU SA to replace the word "should" with "shall".

16. The Board notes that in section II-a-9, regarding the processing of special categories of personal data, the reference to appropriate safeguards, when Article 9(2) of the GDPR provides so, is missing. For example, with respect to the processing, which is necessary for reasons of public interest (Article 9(2)(i) of the GDPR) in the area of public health, the suitable and specific measures provided for by Union or Member State law to safeguard the rights and freedoms of data subjects, in particular professional secrecy must be in place. The Board recommends the LU SA to take into account such safeguards, where necessary throughout this section and modify these criteria accordingly.

17. More in detail, with respect to section II-a-9 referring to Article 9(2)(b) of the GDPR, it is mentioned that "the entity has identified the applicable legal basis and formally assessed its applicability with regard to this processing activity". The EDPB recalls that the controller is authorised for such processing by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and interests of the data subject. The EDPB considers that, without taking into account all the elements of compliance provided by this provision, such as the safeguards adhered to by the controller, the certification body's checks and controls would not be concrete enough, considering that the criterion where the assessment relied on is insufficiently detailed. Therefore, the Board recommends the LU SA to modify this criterion accordingly so to allow the certification body's assessment to be exhaustive.

18. Similarly, concerning the "legitimate activities by a foundation, association or any other non-for-profit body [...]" the Board recommends to take into account the appropriate safeguards required by Article 9(2)(d) of the GDPR.

19. Along the same lines, with respect to Article 9(2)(g) of the GDPR regarding the "substantial public interest" the mere reference in the criteria to the identified Union or Member States law(s) is not sufficient. The "specific measures to safeguard the fundamental rights and interests of the data subject" should also be taken into account and ensured to exist in this context. Therefore, the Board recommends to consider such elements in the draft certification criteria to provide sufficient added value for the certified entities in terms of compliance with the GDPR.

20. Similarly, under the same section, the Board notes that there is no reference to further conditions, including limitations regarding the processing of genetic data, biometric data or data concerning health. The Board recommends that the LU SA modifies this criterion accordingly so as to refer to the elements of compliance with the GDPR pursuant to Article 9(4), where relevant.

21. With regard to section II-a-18 concerning the transfer of personal data to third country, the Board recommends that the LU SA includes a reference to Articles 44-45 of the GDPR in the "Label" field of the draft certification criteria along with the relevant recitals of the GDPR.

22. In addition to the assessment mentioned in criterion II-a-18, the entity should also substantiate the choice made regarding the data transfer mechanism, pursuant to Chapter V of the GDPR. [7] Therefore, the Board recommends that the LU SA takes into account in the draft criteria the need to substantiate the choice made with respect to the data transfer mechanism.

2.6 Principles of Article 5

23. Regarding the purpose of compatibility under section II-b-2, the Board recommends the LU SA to add more details in relation to the elements on which the compatibility assessment of further purposes must be based, at least the ones established by Article 6(4) of the GDPR, as the criteria for the compatibility test listed therein are missing. Regarding section II-c-1, the Board encourages the LU SA to take into account the amount, type and nature of the data collected and processed among the factors to consider as likely to influence the implementation of the principle of data minimisation.

24. With regard to section II-c-2 ", the Board encourages the LU SA to clarify in the context of "less intrusive means" what needs to be demonstrated.

25. Regarding the principle of data accuracy in section II-d-2, the draft certification criteria state that "The entity has defined and implemented a procedure to verify on a regular basis and at least annually the personal data it received, either by directly contacting the data subject, or by contacting the source from which it received the data. The entity documents this verification of data accuracy and has implemented a procedure to update data if necessary" The Board encourages the LU SA not to limit the personal data referred to in these criteria to the ones the entity "received", but also refer to the data it holds in general (e.g. those inferred or created from the data received or otherwise produced by the entity). Furthermore, for reasons of completeness, in the passage "to update data if necessary", the Board encourages the LU SA to add that data will also be corrected or deleted where necessary.

26. Regarding the deletion or anonymisation of data in section II-e-2, the draft certification criteria list certain use cases in which the applicant is required to effectively ensure these operations. In particular, the second and third bullet point mention: "where personal data is not, or no longer necessary for the purpose of the processing; when it no longer needs the data; or". The Boards notes that another use case might be where the SA orders the erasure of personal data under Article 58(2)(g) of the GDPR. In any case, the Board encourages the LU SA to clarify the difference between the two use cases described in these two bullet points or otherwise delete one of them, as well as to take into account in the draft certification criteria other possible use cases, such as the one of Article 58(2)(g).

2.7 General Obligations for Controllers and Processors

[7] In the context of this assessment, the relevant CJEU judgements and the EDPB Guidelines and recommendations should be taken into account.

2.7.1. Obligation applicable to controllers and processor

27. Under section I-11 of the draft certification criteria, regarding the DPO´s competences, the Board notes that if the DPO does not have minimum three years of professional experience, he/she either (i)"needs to have two years of legal experience and has followed comprehensive trainings on data protection" or (ii) "The DPO has access to legal assistance internally, or via a non-limiting service contract with an external firm, covering all GDPR subjects". The Board is of the opinion that the second requirement should not stand alone for the assessment of the DPO's qualification. This means that the DPO should not be considered qualified only because he/she "has access to legal assistance internally, or via a non-limiting service contract with an external firm, covering all GDPR subjects". This could be an additional requirement for the evaluation of DPO's qualifications, but not a stand-alone one. Since the scheme heavily relies on the DPO, it is important that he/she has the appropriate expertise. In addition, the required trainings on data protection should be recent and up to date. Therefore, the Board recommends that the LU SA amends this section accordingly.

28. Under section I-12 of the draft criteria (last point) the LU SA refers to cases where conflicts of interest of the DPO have been identified. The Board welcomes this inclusion, it however considers that the notification to the entity's highest management and the documentation of the conflicts of interest are not enough. It is essential that this conflict of interest is resolved according to an established procedure. Therefore, the Board recommends the LU SA to add this element under this section.

29. The Board notes that, under section I-13 of the draft criteria, the LU SA refers to the obligation of the DPO to "inform and advise the entity and its employees, who carry out processing activities, of their obligations pursuant to the GDPR and to other Union or Member State data protection provisions [...]". The LU SA clarified that this does not refer to data protection provisions of other Member States, but to provisions of national laws and regulations. Therefore, the Board encourages the LU SA to modify this reference accordingly in the criteria.

30. The Board notes that sections I-14 and I-15 of the draft certification criteria are devoted to data breaches: the first one is designed to be applicable to controllers and the second one to processors. In particular, these sections require the implementation of "technical and organisational measures to identify, manage and notify personal data breaches" by the entity seeking for certification. Those measures have to cover various aspects, including the degree of involvement of the DPO. However, in this regard, both criteria seem to be contradictory as, on the one hand, they require that "the DPO should always be informed of each data breach", while, on the other hand, they refer to a "formal procedure" in place defining "when the DPO needs to be informed and what this information shall include". Indeed, it is not clear if these two requirements refer to different factual contexts. Therefore, the Board recommends the LU SA to explain if it this is the case and to solve this contradiction between both sections anyhow.

31. In section I-14, with regard to the notification to the SA, the Board recommends the LU SA to delete the term "if applicable" from the sixth bullet point.

32. Section I-15 of the draft certification criteria, which applies to processors, envisages the implementation of "technical and organisational measures to detect, manage and notify personal data breaches towards the contractual partner(s) and / or controller(s) within a timeframe allowing the controller to notify the supervisory authority within 72 hours". With

regard to the envisaged timing, the Board notes that Article 33(2) of the GDPR requires the processor to notify the personal data breaches to the controller "without undue delay" after becoming aware of it. Therefore, the Board recommends the LU SA to add the term "without undue delay" in relation to the processor's obligation to this section.

2.7.2. Obligations applicable to the controllers

33. The Board notes that section II-f-7 mentions that "The entity reviews the DPIA on a regular basis and at least annually or when significant changes impacting the DPIA occur. The entity takes into account the formal opinion of its DPO". The Board recommends the LU SA to bring this section in line with Article 35(9) of the GDPR, so as to consider the opportunity to seek the views of data subjects or their representatives (without prejudice to the protection of commercial or public interests or the security of processing operations).

34. In relation to the DPIA review in section II-f-7, it is mentioned that this shall be carried out, among others, "when significant changes impacting the DPIA occur". In this regard, the criterion requires the entity to implement "a documented method ensuring that it took into account all factors likely to influence the DPIA" and that "such factors can be external or internal and include among others changes in the applicable regulatory framework […]". In relation to those changes, the Board recommends the LU SA to also add a reference to changes of the risk represented by processing operations as envisaged by Article 35(11) of the GDPR.

35. Regarding section II-f-9 of the draft certification criteria, titled "assessment of sufficiency" which concerns the use of processors by the applicant, the Board encourages the LU SA to take into account the expert knowledge, reliability and resources that the processor needs to have before engaging it, in line with Recital 81 of the GDPR. Furthermore, with regard to the last bulled point of this section, the Board recommends the LU SA to make clear that the audits the controller is required to perform, according to sections II-f-5 and II-f-6 of the draft certification criteria, can be conducted towards the processor.

36. In section II-f-10 regarding a contract / legal act under Union or Member State law, the Board recommends the LU SA to include a reference to the elements that must be set out in this contract/legal act under Article 28(3) of the GDPR, such as the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

37. Moreover, when the draft certification criteria mention that there has to be a contract / legal act under Union or Member State law in place, the Board recommends to specify that, according to Article 28(9) of the GDPR, this should be in writing (including in electronic form) so to be checked by the certification body.

38. With regard to the sixth bullet point of the same criteria, stating: "The processor assists the entity in ensuring compliance with his obligations taking into account the nature of processing and the information available to the processor", the Board encourages to add a reference to the entity's legal obligations which result from Articles 32 to 36 of the GDPR.

39. The criteria in section II-f-12 refer to "due diligences procedures" in addition to audit and monitoring by the applicant towards the engaged processors. The Board notes that the term "due diligence" can be very broad and take on different meanings, depending on the content and structure of the underlying contract, which in turn places special data protection

requirements on the respective audits. Therefore, since the risk of non-compliant implementation is not insignificant and the use of this term can lead to ambiguity about the necessary extent of audits, the Board encourages the LU SA to clarify the term "due diligence procedure" in the draft criteria.

2.7.3. Obligations applicable to processors

40. With regard to Section III of the draft certification criteria, concerning the principles relating to processing of personal data by the processor or the sub-processor, the Board recommends the LU SA to add in section III-1 that the contract or legal act between processor and controller or sub-processor and processor should be in writing (including in electronic form) in line with Article 28(9) of the GDPR.

41. When the same draft certification criteria mention that the entity "assists the contractual partner and the controller in ensuring compliance with his obligations taking into account the nature of processing and the information available to the entity, the Board encourages the LU SA to add an explicit reference to the sub-processor's obligations to assist the processor and the similar obligation of the processor to assist the controller with regard to the obligations of the latter under Articles 32-36 of the GDPR.

42. With regard to section III-3 of the draft criteria, concerning the limitation of the processing to the documented instructions received by the controller or the contractual partner, the Board recommends the LU SA to add a reference to international transfers in line with Article 28(3)(a) of the GDPR.

43. Under section III-11 of the draft certification criteria regarding the assessment of sufficiency, the Board notes that there should be a reference to the processor's obligation to assess the sub-processors it intends to engage.[8] The Board encourages the LU SA to modify this criterion accordingly.

44. With regard to section III-3 of the draft certification criteria concerning the transfer of personal data to third countries, the Board recommends to adjust this criterion to the recommendation set out above as regards section II-a-18.

2.8 Rights of data subjects

45. Under section I-9 of the draft certification criteria "facilitate the exercise of data subjects' rights", the Board takes note of two different scenarios of impossibility of the entity to comply with the request set by controller. The Board understands that the first scenario refers to situations that the entity cannot comply within the deadline set by the controller, while the second refers to an absolute impossibility to comply. However, the distinction between the two scenarios is not clear in the criteria, thus the Board encourages the LU SA to clarify this.

46. With respect to the exercise of the data subject rights, the Board welcomes, in relation to the fees that can be charged by the controller, in case of manifestly unfounded or excessive requests from the data subject, the obligation of the entity to document "how it justifies the amount of the charged fees". This obligation is found in section II-a-10 (right to object) section

[8] Similar obligations are provided in the EDPB Opinion on Article 28 GDPR SCCs, clause 7.6. regarding the authorisation to use a sub-processor "In order to make the assessment and the decision whether to authorise sub-contracting, the data processor shall provide the data controller with all necessary information on the intended sub-processor, including on their locations, the processing activities they will be carrying out and on any safeguards and measures to be implemented."

II-a-11 (right to restriction of the processing), section II-a-12 (right not to be subject to automated individual decision-making), section II-a-16 (right to access) and section II-a-17 (right to data portability). In this regard, the Board notes that the elements to take into account to consider reasonable the amount of the charged fees are specified in Article 12(5)(a) of the GDPR and should not be left to the discretion of the entity seeking for certification or the certification body. Therefore, the Board recommends the LU SA to include a reference to these elements in this section (i.e. the administrative cost of providing the communication or taking the action requested by the data subject).

47. As regards the right of data subject not to be subject to automated decision-making including profiling, the Board notes that "profiling" is included in the title of the relevant Section, II-a-12. However, it is missing from the main text of the criterion (first paragraph). The Board encourages this addition.

48. Moreover, data subjects' right of access is provided under section II-a-16 of the draft certification criteria. However, the draft misses to include the list of information to be provided to the data subject, pursuant to Article 15(1). Therefore, the Board encourages, for consistency with the rest of the draft certification criteria devoted to data subjects' rights, to also refer here to all the obligations provided under Article 15(1) of the GDPR (i.e. the information that the controller should provide to data subjects when they exercise their right of access).

49. Within the same Section, the Board notes that the draft certification criteria do not include that the first time the entity provides a copy to the data subject, this should be free of charge and that for any further copies requested, the entity may charge reasonable fees based on administrative costs. The Board recommends that the LU SA includes this aspect in the criteria.

50. Similarly, the reference to the modalities on how to provide the information requested by the data subject, is missing. The Board recommends to add a clarification thereof that when the data subject makes the request by electronic means, and unless otherwise requested, the information must be provided in a commonly used electronic form.

51. Under the section II-a-17 regarding the right to data portability, an important element to be assessed is missing. In particular, pursuant to Article 20(4) of the GDPR, there is need to assess whether the data subjects' right to data portability adversely affects the rights and freedoms of others. The Board recommends this addition, as this element also need to be assessed by the certification body in the context of the right to data portability.

2.9 Risks for the rights and freedoms of natural persons and technical and organisational measures guaranteeing protection

52. Regarding the sections about the risk analysis, in II-f-2 and III-6 it is not made clear enough which risks are being addressed, namely those of the data subjects. The Board recommends the LU SA to include, among the risks mentioned in this requirement, those to the rights and freedoms of the data subjects. In addition, the Board recommends that the LU SA adds more information regarding the different types of risks with regard to the data subjects concerned.

53. In line with the previous recommendations concerning the risk analysis, the Board recommends the LU SA to also add, in section II-f-3 and III-7, that the risk treatment takes into account the different types of risks to the rights and freedoms of the data subjects concerned.

54. Furthermore, it is mentioned that the entity should consider at least the technical and organisational measures of the access control policy. The Board recommends the LU SA to bring this in line with Article 32(4) of the GDPR by adding the entity's obligation to take steps to ensure that any natural or legal person acting under its authority, who has access to personal data, does not process them except on instructions from the entity, unless he or she is required to do so under Union or Member State law.

55. The draft certification criteria also state in II-f-3 and III-7 that the entity reviews the effectiveness of the risk treatment plan at least on an annual basis or when changes impacting the risk evaluation occur and adapts the risk treatment plan if necessary. The Board encourages the LU SA to make clear that there are processes in place to measure and ensure the effectiveness of the said plan, so as to ensure that the certification criteria are self-explanatory and that the certification body could know what it needs to check from the sole formulation of the criteria.

56. Regarding the implementation of organisational and technical measures the draft certification criteria state in section II-f-4 and III-8 that on a daily basis, reports on controls performed and security incidents related to the processing activities in scope shall be provided at least to the DPO and the entity's management. The Board encourages the LU SA to add that these reports should be provided also to the relevant persons within the organisation who are involved - so not only to the DPO and the entity's management.

3 CONCLUSIONS / RECOMMENDATIONS

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

58. regarding the "scope of the certification mechanism and target of evaluation (TOE)", the Board recommends that the LU SA:

    1) includes specific criteria covering processing activities under Articles 85 to 89 of the GDPR.

    2) includes an analysis of the relevant laws which shall be performed by the entity demonstrating that specific and suitable measures have been put in place in order to respect the fundamental rights and interests of data subjects pursuant to Article 89 of the GDPR

59. regarding the "procedure to determine a target of evaluation (TOE)" the Board recommends that the LU SA:

    1) includes in the beginning of the draft certification criteria, in a devoted section, sufficient information with regard to the criteria on how the ToE is defined .

60. regarding the "certification criteria" the Board recommends that the LU SA:

1) amends the criteria listed in paragraph 10 of this Opinion by providing the factors that shall be taken into account by the applicant when carrying out the relevant assessments so as to also clarify what will be checked by the certification body.

61. regarding the "lawfulness of the processing" the Board recommends that the LU SA:

1) modifies section II-a-I which refers to a "valid legal basis" so as to take into account how the applicability of the legal basis is demonstrated and its appropriateness, where relevant, considering the processing activities, depending on the nature, context, scope and purposes of the processing.

2) in relation to section II-a-3, takes into account that the entity demonstrates the "appropriateness" of consent as legal ground for the processing in the individual case, so to have this criterion in line with Recital 43 of the GDPR and the 05/2020 EDPB Guidelines on consent under the GDPR.

3) in section II-a-3 adds, the minimum requirements which have to necessarily be met so that consent can be considered informed and unambiguous and that the certification criteria bring sufficient added value for the GDPR compliance of the certified entities.

4) takes into account, where necessary, throughout section II-a-9, the appropriate safeguards, as provided by Article 9(2) of the GDPR with regard to the processing of special categories of data, and modify the related criteria accordingly .

5) modifies the criterion under section II-a-9 which refers to Article 9(2)(b) of the GDPR, so as to take into account that the controller must be authorised for such processing by Union or Member State law or a collective agreement pursuant to the Member State law providing for appropriate safeguards for the fundamental rights and interests of the data subject, in order to allow the certification's body assessment to be exhaustive.

(6), takes into consideration, in section II-a-9, the appropriate safeguards, as provided in Article 9(2)(d) of the GDPR regarding the "legitimate activities by a foundation, association or any other non-for-profit body [...].

(7) takes into account, in section II-a-9, the specific measures taken to safeguard the fundamental rights and interests of the data subject with regards to the "substantial public interest" in the context of Article 9(2)(g) of the GDPR.

(8) modifies, in section II-a-9, the criterion so as to refer to the further conditions, including limitations regarding the processing of genetic, biometric and data regarding health, set out in national law pursuant to Article 9(4) of the GDPR, where relevant.

(9) includes a reference to Article 44-45 of the GDPR in the "Label" field of section II-a-18 of the draft certification criteria along with the relevant recitals of the GDPR.

(11) requires, in section II-a-18, that the entity substantiate the choice made with regard to the data transfer mechanisms, pursuant to Chapter V of the GDPR.

62. regarding the "principles of Article 5" the Board recommends that the LU SA:

(1) adds, under section II-b-2, more details in relation to the elements on which the compatibility assessment of further purposes must be based, at least the ones established by Article 6(4) of the GDPR.

63. regarding the "general obligations for controllers and processors" the Board recommends that the LU SA:

(1) modifies the criterion under section I-11, regarding the DPO competences, so to make sure that the (ii) requirement does not stand alone, but is an additional requirement for the assessment of the DPO's qualification and that the required trainings on data protection are recent and up to date.

(2) adds, under section I-12, that when a conflict of interest has been identified, it will be resolved according to an established procedure.

(3) clarifies, in sections I-14 and I-15, the degree of DPO's involvement when, on the one hand, the draft criteria require that "the DPO should always be informed of each data breach", while, on the other hand, they refer to a "formal procedure" in place defining "when the DPO needs to be informed and what this information shall include".

(4) deletes the term "if applicable" from the sixth bullet point of section I-14 with regard to the notification of data breaches to the SA .

(5) adds to section I-15 the term "without undue delay" in relation to the processor's obligation to notify the personal data breach to the controller" after becoming aware of it, pursuant to Article 33(2) of the GDPR.

(6) modifies, in relation to the DPIA review, section II-f-7 to bring it line with Article 35(9) of the GDPR, so as to consider the opportunity to seek the views of data subjects or their representatives (without prejudice to the protection of commercial or public interests or the security of processing operations).

(7) modifies, with regards to factors likely to influence the DPIA, section II-f-7 to include a reference to the changes of the risk represented by processing operations envisaged by Article 35(11) of the GDPR.

(8) modifies the last bullet point of section II-f-9, to make clear that the audits that the controller is required to perform according to the sections II-f-5 and II-f-6 of the draft certification criteria can be conducted towards a processor.

(9) adds, under section II-f-10, a reference to the elements that must be set out in the contract/legal act under Article 28(3) of the GDPR, such as the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

(10) specifies, under section II-f-10 and III-1, that when there has to be a contract/legal act under Union or Member State law in place, according to Article 28(9) of the GDPR, this should be in writing so as to be checked by the certification body.

(11) under section III-3, regarding the limitation of the processing to the documented instructions received by the controller or the contractual partner, includes a reference to international transfers in line with Article 28(3)(a) of the GDPR.

(12) adjusts section III-3 of the draft certification criteria to the recommendation provided for section II-a-18.

64. regarding the "rights of data subjects" the Board recommends that the LU SA:

(1) includes a reference to the elements to be taken into account to consider the reasonable amount of charged fees provided in Article 12(5)(a) of the GDPR in case of manifestly unfounded or excessive requests from the data subject (i.e. the administrative cost of providing the communication or taking the action requested by the data subject).

(2) includes, under section II-a-16, that the first time the entity provides a copy to the data subject, this should be free of charge and that for any further copies, the entity may charge reasonable fee based on administrative costs.

(3) clarifies in the same section that when the data subject makes the request by electronic means, and unless otherwise requested, the information must be provided in a commonly used electronic form.

(4) includes in section II-a-17 that there is need to assess whether the data subjects' right to data portability adversely affects the rights and freedoms of others.

65. regarding the "risks for the rights and freedoms of natural persons" and the "technical and organisational measures guaranteeing protection" the Board recommends that the LU SA:

(1) includes, among the risks mentioned in sections II-f-2 and III-6, those to the rights and freedoms of the data subjects and adds information regarding the different types of risks with respect to the data subjects concerned.

(2) adds, under sections II-f-3 and III-7, that the risk treatment takes into account the different types of risks to the rights and freedoms of the data subjects concerned.

(3) aligns the requirement of the entity to consider at least the technical and organisational measures of the access control policy with Article 32(4) of the GDPR by adding the relevant obligation.

66. Finally, in line with the Guidelines the EDPB also recalls that, in case of amendments of the GDPR-CARPA certification criteria involving substantial changes[9], the LU 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

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

68. According to Article 64(7) and (8) of the GDPR, the LU 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.

[9] 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.

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

70. The EDPB recalls that, pursuant to Article 43(6) of the GDPR, the LU 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

(Andrea Jelinek)