Opinion 25/2022 regarding the European Privacy Seal (EuroPriSe) certification criteria for the certification of processing operations by processors

Adopted on 13 September 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 the 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 “European Privacy Seal (EuroPriSe) certification criteria for the certification of processing operations by processors” (hereinafter the “draft certification criteria” or “certification criteria”) was drafted by the EuroPriSe Cert GmbH (hereinafter the “EuroPriSe ”), a legal entity in Germany and submitted to the Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, the competent German supervisory authority in North Rhine-Westphalia (hereinafter the “DE SA (NRW)”).

2. The DE SA (NRW) has submitted the draft criteria of a national certification scheme to the EDPB and requested an Opinion of the Board pursuant to Article 64(1)(c) GDPR on 2 June 2022. The decision on the completeness of the file was taken on 7 July 2022.

2 ASSESSMENT

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

2.1 General remarks

4. In the opinion of the Board, the scope of the certification scheme is not made sufficiently clear. Notwithstanding the fact that the scope of the scheme is indicated between brackets ("(scope: DE)") on the title page of the document, this page also contains the wording ('European Privacy Seal') which may still give the impression that the scheme has a European scope. Therefore, the Board encourages to make the scope of the certification scheme clear in the introductory text of the document.

5. The present certification is not a certification according to Article 46(2)(f) of the GDPR meant for international transfers of personal data. It 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.

2.2 Processing operations by a processor

6. In the view of the Board, the assessment whether the applicant is a processor is part of the application review (and not of the criteria pursuant to Article 42(5) of the GDPR). The certification body must assess the role based on the information and documents provided by the applicant when applying for a certification. Therefore, the Board recommends to leave section 1 out of the criteria pursuant to Article 42(5) of the GDPR and incorporate it to the application process.

7. The Board also notes that the current scheme provides for criteria pursuant to Article 28 GDPR to be met in the relationship of the processor with the controller (in section 2.2 of the scheme) and in the relationship of the processor with other processors[4] (sub processors) (in section 2.3.3 of the scheme). In order to make clear that this does not imply that such sub-processor can be certified under this scheme and that only the processing operations performed on behalf of the applicant is subject to certification, the EDPB recommends to clarify also in the introduction that sub processors cannot be certified under the EuroPriSe certification scheme.

2.3 Requirements from a legal perspective

[4] Other processors within the meaning of article 28 (2) and (4) of the GDPR.

2.3.1 Record of processing activities

8. The requirement to maintain a record of processing activities pursuant to Article 30 (2) of the GDPR is stipulated in section 2.1.1. of the certification criteria. According to EuroPriSe, this requirement "will be applicable as a rule". However, the Board encourages to clarify whether the exemptions of Article 30 (5) of the GDPR could still apply in individual cases or if – in order to meet the criteria in the EuroPriSe scheme – such a record of processing activities must always be maintained by a certification customer regardless of the exemptions.

2.3.2 Applicants subject to Article 3.2 GDPR

9. The Board notes that according to section 2.1.3., processors who do not have an establishment in the European Union (EU) or in the European Economic Area (EEA) shall designate a representative in accordance with Article 27 of the GDPR. Consequently, the Board understands that the EuroPriSe certification scheme is applicable for certification customers that are established outside the EU or the EEA.

10. Since this could imply that such a processor established outside the EU/EEA could also process personal data outside the EU/EEA, the Board recommends to clarify in section 2.1.3. that whenever a "transfer" within the meaning of Article 44 of the GDPR to a processor established outside the EU or the EEA takes place, the obligations stipulated in Chapter V of the GDPR must be fully respected. Furthermore, the Board recommends to clarify in section 2.1.3. that the present scheme is not a scheme pursuant to Article 46 (2)(f) GDPR. The Board recommends to clarify in section 2.1.3. that the applicant is not entitled to make use of the certification in a way that could give the impression that the certification itself is a transfer tool pursuant to Article 46 (2)(f) GDPR. Data controllers should, irrespective of the presence of the certification seal, nonetheless perform an assessment of the legislation of the host country before transferring data to the non-EU GDPR certified processor. In case the legislation does not provide for the appropriate level of protection, supplementary measures should be put in place.[5]

11. A data processor should refrain from applying for certification if they are aware that their legislation would prevent them from complying with the GDPR principles enshrined in the certification scheme.

2.4 Relationship controller-processor

12. The Board notes that under section 2.2 and 2.3 of the EuroPriSe certification criteria, reference is made to the requirements with regard to Article 28 GDPR. Section 2.2.1 of the certification criteria deal with the existence of contractual clauses that meet all the requirements of Article 28 GDPR. In this regard, the Guidance states that the processor draws up a Data Processing Agreement (DPA) template that meets all the requirements of Article 28 GDPR. Notwithstanding the fact that the guidance also mentions that the template does not have to be used, the Board encourages to provide additional wording in this guidance to clarify that such a Data Processing Agreement template is without prejudice to the right of the data

[5] See EDPB 01/2020 Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer.

controller to provide or negotiate the Article 28 GDPR clauses with the data processor without consequences on the certification.

13. Furthermore, section 2.2.1 mentions that this requirement "must be modified if the respective processing by a processor on behalf of the controller is not based on a contract but on another legal instrument under Union or Member State law." However, when other legal instruments are in place, the requirement of section 2.2.1 is not applicable. In these cases such contractual clauses are not required. The Board recommends to modify the wording accordingly.

14. Section 2.2.1 instructs the Certification Body to examine "whether the relevant legal instrument complies with the requirements of Art. 28 GDPR", accompanied by a footnote which explains that "this constellation is not considered in more detail in this v2.1 of the criteria catalogue due to lack of practical relevance". When certain criteria lack practical relevance, they should not be part of the criteria catalogue. The Board therefore recommends to delete these sentences from section 2.2.1.

15. The requirement in section 2.2.1, point 2 e) of the criteria in detail should not just repeat the text of Article 28, but instead the Board recommends to further specify the assistance that the processor should or could offer for the fulfillment of the controller's obligation to respond to requests for exercising data subject rights. This, in order to reflect the actual operational options the processor and the controller have, i.e. to what extent the controller is practically dependent on the assistance of the controller for the exercise of data subject rights (support being imperative) or the controller merely prefers (some kind of) support from the processor on this issue (support being elective). The requirement should also stipulate that such clauses should be in line with the GDPR responsibility of the controller regarding data subject rights and not unduly transfer this responsibility to the processor.[6] The EDPB recommends to modify requirement 2.2.1 so that it is taken into account to what extent the controller is actually dependent on the processor for the assistance of the processor regarding data subject rights.

16. Section 2.2.2 (point 8 of the criteria in detail) states that the processor provides all "necessary information" to demonstrate compliance with Article 28 GDPR. It is not completely clear what documents this requirement is specifically referring to, as the list of documents is open ended, and the term "necessary information" rather vague. The Board therefore recommends to identify an exhaustive list of documents/information that has to be checked by the Certification Body to verify if this criteria is fulfilled or not. Furthermore, this criterion should clarify that this documentation/information shall be provided to the Certification Body.

17. Section 2.3.2 states that "the processor shall have concluded contracts with all other processors that impose the same data protection obligations as set out in the contract(s) between the controller(s) and the processor on that other processor". To enhance to readability, the Board encourages to slightly modify the last part of the sentence. For example, "on that other processor" could be changed into "sub-processor".

18. Section 2.3.2 (point 1a of the requirement in detail) states that the exact time period or the criteria according to which it is determined shall be specified. For reasons of clarity, the Board recommends to include in this requirement that these specifications on the duration of the

[6] This paragraph should be read this in conjunction with paragraph 35, 36 and 37.

processing shall be in accordance with the relevant provisions of the data processing agreement between the controller and the processor.

2.5 Requirements for specific types of processing operations

2.5.1 Statutory confidentiality obligations, professional secrets and special official secrets not based on statutory provisions

19. The Board notes that the requirement stipulated in section 2.4.1. "is only applicable if the processing operations to be certified are exclusively resp. mainly used by controllers who are subject to special confidentiality / secrecy obligations." In the view of the Board, it is unclear whether this requirement applies in case only "few" controllers that are subject to special obligations use the processing operations of the certified processor. Furthermore, it is unclear in which circumstances the term "mainly" is fulfilled. Therefore, the Board recommends to clarify section 2.4.1 accordingly.

20. In addition to footnote 63 of the EuroPriSe certification scheme, the Board encourages to provide further examples in the "Guidance" of section 2.4.1. regarding how a contract template for a data processing agreement could address specific confidentiality obligations under EU law or Member State law.[7]

2.5.2 Transfer of personal data to third countries

21. The Board notes that section 2.4.2 stipulates requirements regarding Chapter V of the GDPR. However, the EuroPriSe certification is not itself a transfer instrument for transfers of personal data to third countries or international organisations pursuant to Article 46(2)(f) of the GDPR. In this context, the Board recommends to clarify in section 2.4.2 that the EuroPriSe certification scheme itself is not a transfer instrument according to Article 46(2)(f) of the GDPR, as it 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). In addition, the Board recommends to include the obligation of the certification applicant to inform the controller about the fact that the EuroPriSe certification scheme itself is not a transfer instrument according to Article 46(2)(f) of the GDPR.

22. Furthermore, the Board recommends to clarify in section 2.4.2 that these specific requirements are only applicable when the certification applicant (as processor) is transferring personal data to a data importer in a third country and to stipulate a requirement for certification applicants to substantiate and document their choice for a particular transfer tool pursuant to Chapter V of the GDPR.

23. Section 2.4.2.1 stipulates general requirements regarding the transfer tools of Chapter V of the GDPR.[8] In the view of the Board, such general requirements are not auditable and could lead to inconsistencies in the application of the EuroPriSe certification scheme. While there

[7] The examples could be similar to the "use cases" of section 2.4.2.1.

[8] *« Here, it SHALL be assessed (and documented) on a case-by-case basis and, as the case may be, in collaboration with the importer (recipient of the personal data in the third country), if there is anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards contained in the transfer tools under Art. 46 GDPR. If this is the case, the processor SHALL implement (and document) supplementary measures that fill these gaps in the protection and bring it up to the level required by EU law. In this respect, technical measures, organisational measures and additional contractual measures can be considered, whereby it may be necessary to combine several of these measures in individual cases. »*

are “use cases” to give examples on the application of the EuroPriSe certification scheme, the Board notes that according to EuroPriSe, such “use cases” and “guidance” are not part of the normative criteria. Therefore, this Opinion does not contain conclusions on the correct application of the GDPR in the “use cases” that are provided in section 2.4.2.

24. As a result, since the uses cases address supplementary measures, the Board recommends to include more specifications regarding the assessment of compliance with the data exporter obligations stipulated in Chapter V. In particular, regarding the implementation of supplementary measures, the EDPB Recommendations on measures that supplement transfer tools shall be referred to in the criteria.[9]

25. Finally, the Board notes that section 2.4.2.1. stipulates requirements regarding Article 49 of the GDPR. In this context, the Board recommends to include a requirement of the applicant to provide specific information to the certification body as to which situations and under which conditions the applicant would rely on the exemption of Article 49 of the GDPR.

2.6 Data protection by design and by default

26. Section 2.5.3 states that this requirement does not apply to processing operations by processors that are used by the principals (controllers) for *many* different purposes. The term ‘many’ is too open to be used by a Certification Body to verify conformity. The Board therefore recommends to give more a precise indication of when this requirement is applicable and when it is not, by for instance quantifying the amount of purposes that make it impossible to apply this requirement (for example: “three or more purposes”).

27. In subsection 2.5.3.1 the controller is obliged to use a leaflet which contains information on relevant data protection aspects. Under point 2, it is stated that the leaflet shall contain information on the designation of potential legal bases on which the controller can rely, as the case may be. The Board recommends to delete this point from the criteria catalogue, as it interferes with the responsibility of the controller to define the appropriate legal basis and ensure that all conditions for this legal basis are met. This is without prejudice to the obligation of the processor to immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions, pursuant to Article 28 (3) GDPR.

28. Subsection 2.5.3.1 contains the obligation for the processor to have designated the support services with regard to responding to requests for the exercise of data subject rights in the leaflet. For clarification reasons, and to align with Article 28 (3) (e) GDPR, the Board encourages to modify this sentence as follows: “Designation of the services of the processor with regard to assist the controller in responding to requests for the exercise of data subject rights…”.

29. Subsection 2.5.3.2 contains an obligation to draw up a model form for a declaration of consent or to release from confidentiality if consent is the only legal basis for the use of the processing operations to be certified. The same obligation applies if the processing operations to be certified involve a transfer of personal data to third countries and if consent serves as the legitimation for said transfer. Although such a model might be helpful for some controllers, in

[9] See EDPB 01/2020 Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer.

particular small and medium sized enterprises, the Board recommends to delete this specific requirement, as acquiring consent is not the responsibility of the processor but of the controller, and thus cannot serve as a criteria for the processor to demonstrate compliance with the GDPR, which, in the end, is the purpose of GDPR certification.

2.7 Technical and organisational measures

30. The Board notes that referring to the risk analysis in section 3.1.1.1. and 3.1.5.1, it is not entirely clear which risks are being addressed (e.g. those of the data subjects). The Board therefore recommends specifying that the risks to the rights and freedoms of the data subjects are addressed. Furthermore, the document refers in the guidelines of several requirements to a classification of risks, however, in none of the requirements a clarification of this classification has been made. For the sake of clarity, the Board therefore recommends adding in Section 3.1.1.1 and Section 3.1.5.1 a reference to the classification of risks regarding the different types of risks with regard to the data subjects concerned.

31. In section 3.1.1.3, the Board acknowledges the intention of EuroPriSe to highlight the importance of implementing access control mechanisms when interacting with web-based services. However, the current wording "*this is particularly ensured when interacting with web-based services"* might indicate that these control mechanisms are not as important or obligatory in all other cases. The Board therefore encourages to either delete this sub sentence or rephrase it accordingly.

32. The requirement in section 3.1.2.1. stipulates the processor's obligation to demonstrate that "the storage duration of the log data can be configured resp. is actually configured in consideration of the existing resp. assumed risk". However, the Board notes that according to Article 5 (1)(c) of the GDPR, the storage duration needs to be adequate, relevant and limited to what is necessary in relation to the purposes for which the data is being processed. The Board therefore encourages adding a reference to consider not only the risks but the purpose of the processing as well.

33. The Board furthermore notes that the "Requirement in a nutshell" in section 3.1.2.1 and section 3.1.2.2. are identical, although the requirements "in detail" deal with different aspects. For the sake of clarity, the Board encourages to consider this differentiation in the "*requirements in a nutshell*" as well.

2.8 Rights of the data subjects

34. As a consequence of the recommendations made by the Board on sections 2.2.1 and 2.2.2 pertaining to contractual clauses on the assistance to be provided by the processor to the controller to facilitate the exercise of data subjects rights, the Board also recommends to reflect and take into account such relevant differences in the contractual clauses in Chapter IV of the EuroPriSe scheme. Also the Board recommends to modify the same approach reflected in the requirements (4.1-4.8) for all the data subjects rights (4.2-4.8), generally phrased as an obligation for the processor to implement 'technical and organizational measures' without any further specification of such measures. Such modifications should reflect the significant differences in the various data subjects' rights, since some of those rights will always be applicable (a), some will depend on a further legal assessment of the situation (b) and some will depend on a substantial appreciation (c). Consequently

responsibilities of the controller and the processor pertaining to (b) and (c) will have to be clarified in the contractual clauses.

35. The requirement in section 4.1 is unspecific as to 'which information is relevant with regards to the controllers' information obligations towards data subjects' that shall be provided by the processor. The Board recommends a further specification taking into account the elements mentioned in Articles 13 and 14 of the GDRP.

36. Regarding the requirement in section 4.8, the Board considers that the controller is in charge of deciding the purposes and means of the processing, and it would therefore appear to be out of the sphere of the responsibility of a processor. Therefore, the Board recommends to further specify which kind of support the processor should provide with regards to the exercise of the right not to be subjected to a decision based solely on automated processing, including profiling.

3 CONCLUSIONS / RECOMMENDATIONS

37. By way of conclusion, the EDPB considers that the EuroPriSe 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:

38. regarding the "scope of the scheme", the Board recommends:

    1) to leave out section 1 of the criteria pursuant to Article 42(5) of the GDPR and incorporates it to the application process.

    2) to clarify in the introduction that sub processors cannot be certified under the EuroPriSe certification scheme.

39. regarding the "applicants subject to Article 3.2 GDPR", the Board recommends:

    1) to include a reminder in section 2.1.3. that whenever a "transfer" within the meaning of Article 44 of the GDPR to a processor established outside the EU or the EEA takes place, the obligations stipulated in Chapter V of the GDPR must be fully respected.

    2) to clarify in section 2.1.3. that the present scheme is not a scheme pursuant to Article 46 (2)(f) of the GDPR GDPR.

    3) to clarify in section 2.1.3. that the applicant is not entitled to make use of the certification in a way that could give the impression that the certification itself is a transfer tool pursuant to Article 46 (2)(f) GDPR.

40. regarding the "relationship controller-processor", the Board recommends:

    1) to adjust the wording of the requirement of section 2.2.1 so that it is clear that when other legal instruments are in place, the requirement of Section 2.2.1 is not applicable.

    2) to delete sentences in section 2.2.1 with regard to a "lack of practical relevance".

3) to modify requirement 2.2.1 so that it is taken into account to what extent the controller is actually dependent on the processor for the assistance of the processor regarding data subject rights.

4) to identify an exhaustive list of documents in section 2.2.2 (point 8 of the requirement in detail) that has to be checked by the Certification Body to verify if this criteria is fulfilled or not. Furthermore, this criterion should clarify that this information shall be provided to the Certification Body.

5) to include in section 2.3.2 (point 1a of the requirement in detail) that the specifications on the duration of the processing shall be in accordance with the relevant provisions of the data processing agreement between the controller and the processor.

41. regarding the "statutory confidentiality obligations, professional secrets and special official secrets not based on statutory provisions", the Board recommends:

1) to include an explanation of the term "mainly used by controllers" in section 2.4.1.

42. regarding the "transfer of personal data to third countries", the Board recommends:

1) to include a reminder in section 2.4.2 that the EuroPriSe certification scheme itself 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).

2) to include the obligation of the certification applicant to inform the controller about the fact that the EuroPrise certification scheme itself is not a transfer instrument according to Article 46(2)(f) of the GDPR.

3) to clarify in section 2.4.2 that these requirements are only applicable when the certification applicant (as processor) is transferring personal data to a data importer in a third country and to stipulate a requirement for certification applicants to substantiate and document their choice of a particular transfer tool pursuant to Chapter V of the GDPR.

4) to include more specifications regarding the assessment of compliance with the data exporter obligations stipulated in Chapter V. In particular, regarding the implementation of supplementary measures, the EDPB Recommendations on measures that supplement transfer tools shall be referred to in the criteria.

5) to include the requirement in Section 2.4.2 that the certification applicant must provide specific information to the certification body in which situations and under which conditions he would rely on the exemption of Article 49 of the GDPR.

43. regarding data protection by design and by default, the Board recommends:

1) to give more a precise indication of when the requirement of section 2.5.3 is applicable.

2) to delete from the criteria catalogue in subsection 2.5.3.1 under point 2, the part in which is stated that the leaflet shall contain information on the designation of potential legal bases on which the controller can rely.

3) to delete from subsection 2.5.3.2 the obligation to draw up a model form for a declaration of consent or to release from confidentiality if consent is the only legal basis for the use of the processing operations to be certified.

44. regarding "technical and organisational measures", the Board recommends:

1) to specify in section 3.1.1.1. and section 3.1.5.1 that the risks to the rights and freedoms of the data subjects are addressed.

2) to include in section 3.1.1.1 and section 3.1.5.1 a reference to the classification of risks regarding the different types of risks with regard to the data subjects concerned.

45. Regarding the rights of data subjects, the Board recommends:

1) to reflect and take into account such relevant differences with regard to the assistance of the processor (see recommendations on sections 2.2.1 and 2.2.2) in the contractual clauses in Chapter IV of the EuroPriSe scheme.

2) to modify the same approach reflected in the requirements (4.1-4.8) for all the data subjects rights (4.2-4.8), generally phrased as an obligation for the processor to implement 'technical and organizational measures' without any further specification of such measures.

3) to further specify requirement 4.1 (right to information) taking into account the elements mentioned in Articles 13 and 14 of the GDRP.

4) to further specify which kind of support the processor should provide in requirement 4.8.

4 FINAL REMARKS

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

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

48. The EDPB recalls that, pursuant to Article 43(6) of the GDPR, the DE SA (NRW) shall make public the 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)