Opinion of the Board (Art. 64)

Opinion 15/2023 on the draft decision of the Dutch Supervisory Authority regarding the Brand Compliance certification criteria

Adopted on 19 09 2023

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 ''Brand Compliance certification standard'' (hereinafter the "draft certification criteria" or "certification criteria") was drafted by Brand Compliance B.V. (hereinafter ''Brand Compliance''), a legal entity in the Netherlands and submitted to the Dutch SA (hereinafter the ''NL SA'').

2. The NL SA has submitted its draft decision approving the Brand Compliance certification criteria, and requested an Opinion of the EDPB pursuant to Article 64(1)(c) GDPR on 26 April 2023. The decision on the completeness of the file was taken on 4 July 2023.

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

4. 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.

2.1 GENERAL REMARKS

5. As a general remark, the Board notes that several criteria are phrased in too general terms, which may lead to confusion as to what needs to be audited by accredited certification bodies and how. In particular, the Board considers that certain criteria do not allow for repeated and consistent assessment by several accredited certification bodies. For example, in Section 6.1.2.b, it is not clear from the criterion how the certification body will verify that the applicant has satisfied the conditions for unambiguous consent. In this respect, the Board is of the opinion that the applicant must not only provide a statement that it respects the unambiguous nature of consent, but also provide material evidence of clear affirmative action from the data subjects (e.g. no pre-ticked boxes, written or oral statement, online proactive action from the data subject etc.) as well as proof of implementation of a procedure guaranteeing that consent is implemented as decided (e.g. interviews with data subjects, result of test panels carried out by the controller, etc.). The Board therefore recommends ensuring that each certification criterion is designed in such a way as to enable reproducible assessment by several certification bodies in a consistent manner.

   This applies, inter alia, to the criteria listed below:

   - In Section 5.3.2 ('Data Protection Officer (DPO)'), the criteria on how to demonstrate that the DPO has expert knowledge of data protection and practice (Section 5.3.2.1.b), is consulted in the timely manner (Section 5.3.2.2.a), has active support from the Board (Section 5.3.2.2.b), or that the internal organization is aware of the existence of the DPO (5.3.2.2.d);

   - In Section 6.1.2 ('lawfulness'), the criteria in relation to the lawfulness of the processing, such as how the organization can demonstrate that the conditions for consent are met in practice (Section 6.1.2.b) or the processing pursues a legitimate interest in respect of the data subjects' rights and freedoms (Section 6.1.2.g);

   - In Section 6.2.3 ('data minimisation'), the different possible processing scenarios envisaged by the organization should be provided;

6. The Board recalls that, in accordance with Article 43(6) GDPR, the Brand Compliance draft certification criteria must be made public by the supervisory authority in an easily accessible form. Therefore, the Board encourages that the copyright statement in this document be amended to clarify that the document will be made public by the supervisory authority in accordance with Article 43(6) GDPR.

7. Although the introductory part of the draft certification criteria specifies that Brand Compliance is a national certification mechanism referred to in the first sentence of Article 42(5) GDPR, the Board is of the view that the national scope of the criteria is not entirely clear in the criteria. In particular, the Board notes that the draft certification criteria includes multiple references to Member States "law'' or "additional requirements", for instance in Sections 5, 6, 7 and 8 and to the impact of the processing operations on data subjects in more than one Member State, for instance in sections 6.1.2.c and 8.2.1 of the scheme. According to the Board, this can lead to confusion as to the scope of the certification criteria. Consequently, the Board recommends clarifying the scope of Brand Compliance as a national certification scheme[4].

8. The Board notes that the introduction refers to the obligation for the organisation to meet all the criteria contained in the Brand Compliance certification criteria ''*unless* [it] *can demonstrate that the exclusions have no impact on the organisations ability to comply with the GDPR and this Standard*''. In this respect, the Board reiterates that none of the criteria set out in the certification scheme should simply be disregarded by the applicant, even if it claims to demonstrate its ability to comply with the GDPR in an alternative way. Although in some instances the applicability of certain criteria could be assessed by the applicant due to, for example, the scope of the ToE or the applicability of specific requirements under the GDPR (such as the appointment of a DPO), an assessment of these criteria should be carried out by the applicant and reviewed by the certification body. Therefore, the Board recommends to remove this sentence from the draft certification criteria.

9. The Board notes that the terminology used to name the certification criteria can be misleading as the title refers to "certification standard" and there is no reference to the word "criteria" as referred to in Articles 42(5) and 64(1)(c) of the GDPR. Therefore, the Board encourages to replace the term ''standard'' by ''criteria'' throughout the document.

10. The Board would welcome clarifications as to the meaning of some of the terms in Section 3.1 ('Terminology') by referring, where applicable, to the corresponding definition set out in Article 4 GDPR. For example, instead of explaining that ''the term has the meaning as set out in the GDPR'' the Board encourages to refer directly to the definitions in Article 4(7) for ''controller'', Article 4(8) for ''processor'', Article 4(11) for ''consent'', Article 4(12) for ''personal data breach''.

11. In addition, the Board notes the definition of ''requirement'' in Section 3.1 ('Terminology') as ''*rule or legal obligation, agreement, need or legitimate expectation regarding the target of evaluation*''. However, the Board is of the opinion that it is unclear whether the use of the term ''requirement'' in Sections 4.2, 5.2.1, and ''internal and external requirement'' in Sections 3.1, 7.2.e, 7.2.f and 9.2.1.b, refers to technical and organisational measures (TOM), or additional data protection objectives. Therefore, the Board encourages clarifying the definition and the use of the term ''requirement'' throughout the draft certification criteria.

[4] See Articles 42(4), 55 and 56 GDPR.

12. For the sake of consistency, the Board also recommends to adjust terminology used in the requirements to the one in the GDPR. This applies, in particular, to the following terms:
    - In Section 6.1.2.b, point c), of the certification criteria the terms ''can be freely given" should be replaced by ''is freely given''.
    - In Section 6.1.3.b, the certification criteria refers to "the intake" and to "scope" of personal data while the GDPR refers to the "collection of personal data";
    - In Section 6.1.4.c, the terms "further processing" and "not further processed" should be used instead of respectively "repeated use of personal data" or "frozen";
    - In Section 8.6.g, the term ''consent'' should be replaced by ''authorisation'' in accordance with Article 28(2) GDPR;
    - In Section 8.4.8.b and 8.4.8.c., the term "[…] fully automated individual decision making" should be replaced by "[…] decision based solely on automated processing" instead in accordance with Article 22(1) GDPR.
    - Point 8.4 refers to the "right to restrict processing" instead of "right to restriction of processing".

13. The numbering of the sections or some redirections to other sections of the certification criteria is sometimes inaccurate (e.g. note 2 under Section 6.1.2.d, Section 6.1.5, Section 6.4, Section 6.5, Section 7.4.a,). The Board therefore recommends to rectify the numbering of these sections accordingly.

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

14. The Board notes that Section 4 contains criteria on how to define the ToE. In particular, Section 4.2.a sets out criteria for the organisation to determine and document the applicability of the GDPR, for which ''*exclusion of implementation criteria shall be justified*''. In this regard, the Board recalls that the application or not of a specific criterion remains a decision from the certification body, not the applicant. Consequently, the Board recommends that this sentence be deleted from the draft certification criteria.

15. The Board notes that the certification criteria do not clearly indicate whether sub-processors can be certified under the scheme. In particular, the certification criteria do not entail specific criteria dedicated to sub-processors. In cases where the applicant to the scheme is a sub-processor, the Board considers that Section 8.6 would not be applicable. For example, in a sub-processing relationship, a sub-processor applying for certification would be conducting processing activities instructed by a processor and it would not necessarily be able to demonstrate that the instructions received originate from the controller as suggested under Section 8.6. Similarly, a sub-processor should have a dedicated obligation to inform the processor which is distinct to the obligation of information of Section 8.6.c. Moreover, in case of a data breach, Section 8.8.4 would not be applicable and there should be specific criteria adapted to the certification of sub-processors where the processor shall be notified by the sub-processor. In case sub-processors are eligible to certification, the Board recommends that specific criteria are developed to take into account the specificities of sub-processing. Alternatively, to make clear that sub-processors are outside the scope of this scheme the Board recommends to expressly indicate in the introduction that sub- processors cannot be certified under the Brand Compliance certification scheme.

16. The certification criteria are part of a general certification scheme applicable in the Netherlands, as referred to in Article 42(5) GDPR, and it therefore does not focus on a specific sector or type of processing activities. According to the information provided, the targeted audience consists of organisations ''*in their role as controllers or processors, regardless of their type, size or the processing carried out in the framework of the products and services they provide*''. The Board considers that the scope could be further specified by referring to ''controllers, processors, joint controllers [and, if applicable, sub-processors][5]'' as well as the ''type of product and services'' provided by them and recommends to amend the introduction accordingly.

17. The Boards notes that Section 4 does not contain specific criteria regarding the identification of all data processing activities that would fall within the scope of the certification when defining the ToE. The Board highlights the fact that the description of the ToE should also include details on the role of the actors involved in the processing activities (e.g. data controller, data processor, joint-controller), as well as information on potential data transfers outside of the EU/EEA. The Board understands that some of these criteria have been developed under Section 4.2 and 4.3. However, the Board recommends to clarify that these criteria are to be assessed at an early stage when defining the ToE under Section 4.1.

18. Under Section 4.3, the certification criteria suggest that the duty to determine the scope of the certification lies on the applicant. Similarly, under Section 4.3.c the criteria suggest that it is the task of the applicant's management to approve the ToE and the scope of the certification. The Board highlights that the role of the applicant consists of precisely describing the intended scope of the certification and the ToE in its application for certification so they can be evaluated by a certification body. However, the applicant is not in charge of validating the scope of the criteria. The role of the applicant is limited to describing and proposing the scope of the certification mechanism and the ToE, whereas the certification body is to decide whether they are suitable for certification. The Board recommends to clarify that the decision on the determination of the scope of the certification and the ToE lies on the certification body after being suggested and described by the applicant.

19. In Section 5.3.2.1.d, the Board encourages to clarify that the organisation shall register the DPO with the Dutch Supervisory Authority given the national scope of the certification criteria.

2.3 LAWFULNESS OF PROCESSING

20. Under Section 6.1.2 ('Lawfulness'), the Board notes that the organisation shall ''*determine that processing is allowed because at least one of the following conditions* [for lawfulness] *have been met*''. In this regard, the Board considers that it should be made clear in the draft certification criteria that only one legal basis needs to be chosen and complied with from those listed in Article 6 GDPR. In addition, the Board is of the opinion that the certification criteria should include the requirement to demonstrate the applicability of the legal basis and its appropriateness, where relevant, considering the processing activities, depending on the nature, context, scope and purposes of the processing. The Board therefore recommends to amend Section 6.1.2 accordingly.

[5] See Recommendation under paragraph 15 of this Opinion.

21. The Board notes that some of the criteria in relation to consent are duplicated in Sections 6.1.2.b and 8.3.1.1.b. For the sake of clarity, the Board encourages to make clear links between the criteria instead of duplicating them. In addition, in Section 6.1.2. b ('Consent'), the Board recommends to add requirement with regard to children's consent in this section (for instance by referring to Section 8.3.1.1 in Section 6.1.2.c) as the conditions applicable to child's consent in relation to information society services is also one of the conditions to ensure lawfulness of the processing.

22. The Board notes that Section 6.1.2.c ('performance of the contact') includes the requirement for the processing ''*to be related to the achievement of the main purpose of the contract, and not to any related interests of the organisation*''. The Board encourages to clarify this sentence by stating that the processing should not go beyond the purpose that is integral part of the performance of the contract.

23. With regard to Section 6.1.2.h referring to Article 9 and 10 GDPR, the Board recommends to refer expressly to the conditions set out in these articles under which the prohibition does not apply.

2.4 PRINCIPLES OF ARTICLE 5

24. With regard to Section 6.1 ('Principles relating to the processing activities'), the Board notes that the use of the terms ''principles of the GDPR'' may be confusing and encourages to refer more specifically to the ''principles in article 5 GDPR''.

25. In addition, the Board notes that point 6.1.a ("Policy regarding the principles") provides that the DPO must be consulted on the correct application of the principles in the case of new processing operations and substantial changes to existing processing operations. However, the Board observes that consultation of the DPO should not be limited to these cases. In the Board's opinion, the DPO, where appropriate, should also be consulted to assess the adequacy of the policy established on the application of these principles in accordance with Section 5.2.1.a. The Board encourages to clarify the role of the DPO in relation to these principles accordingly.

26. The Board notes that under Section 6.1.1 of the certification criteria, "*further processing for archiving in the general interest, for scientific or historic research, or statistical purposes is not considered to be incompatible with to the original purposes".* The Board recommends to clarify 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[6]. 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 Section 6.1.1.c, point 3 (i), (ii) and (iii). Accordingly, the Board recommends adding a specific criterion in this respect in Section 6.1.1c, point 3 (i), (ii) and (iii).

27. In Section 6.1.1.d ('Necessity, proportionality and subsidiarity'), the Board encourages to clarify the requirements in this section, in particular their link with the principles under Article

[6] See Recital 156 and Article 89(1) of the GDPR.

5 GDPR, as well as their interaction with the criteria related to the identification of a legal basis.

28. With regard to Section 6.1.1.1 ('Transfer of personal data to a third party'), the Board encourages that, in order to avoid any confusion with the notion of international transfer of personal data under Chapter V, the term ''data transfer'' be replaced by ''data sharing'' or ''data transmission''.

29. In Section 6.4.1 on ''Data minimisation'' the Board recommends to clarify, in accordance with Recital 39, that data minimisation principle requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. As regards Section 6.1.4.b ('Accuracy with repeated use'), the Board recommends to clarify the requirement "longer period of time" in order to allow the applicant to make an objective assessment of its compliance with this criteria.

30. In Section 6.1.5. ('Storage limitation'), the Board recommends to include the obligation for the organisation to ensure deletion by processors to whom data has been shared or transmitted, in accordance with Article 28(3)(g) GDPR. In addition, the Board recommends to remove reference in Section 6.1.5.a that ''*the retention period [...] may be indefinite*'' considering that personal data retention period should be determined in all cases. As regards Section 6.1.5 c ('Anonymisation'), the Board encourages the scheme owner to also include a reference to the cases in which anonymisation is carried out for the purposes of statistical or research purposes as per Article 89(1) GDPR. Finally, the Board notes that another use case leading to the deletion of data might be where the SA orders the erasure of personal data under Article 58(2)(g) GDPR and encourages to include this in the criteria.

2.5. GENERAL OBLIGATIONS FOR CONTROLLERS AND PROCESSORS

31. The Board notes that Section 6.2.a ('Assessing the processing instructions') may be subject to misinterpretation, as the sentence "*the organisation shall, where possible given the nature of the processing operation, establish, document and implement a process [...]*" could be understood as it is at the discretion of the processor to act in such a way. Therefore, the Board recommends to delete "where possible".

32. Regarding Section 6.5.1 ('Joint controllers') the Board notes that a data controller can submit to the Brand Compliance certification process a ToE which is subject to joint-controllership. In case the ToE is subject to joint-controllership, the Board wishes to underline that the accredited certification body will have to carefully conduct the application process to ensure that the ToE is meaningful and that the applicant is fully responsible for the compliance of the ToE with all obligations under the GDPR that the certification mechanism aims at demonstrating. As a consequence, the arrangement concluded between the applicant and the other joint controllers involved in the ToE with regards to their respective responsibilities for compliance with the obligations under the GDPR might – depending on the context of the processing activities of the ToE - prevent the applicant to fulfil the criteria of certification. In this regard, while Section 6.4.1.c ('Evaluating the arrangements') notes that in such situations all controllers "*can only be certified as a whole in order to be meaningful to the target group*". Likewise, Note 3 under Section 4.3.a states that "*Processing operations for which several parties are joint controllers [...] the ToE must cover the processing operations of the joint controllers*", it remains unclear what this means for the certification process as such.

Therefore, when defining the ToE, the Board recommends to define the requirements to be met regarding the arrangement concluded between the applicant and the other joint controllers involved in the ToE with regards to their respective responsibilities for compliance with the Brand Compliance certification criteria. Moreover, the Board recommends to include in Section 6.4.1.b ('Embedding the arrangements') criteria that implement the provisions of Article 26 (3) GDPR.

33. Regarding Section 8.8.4 ('Notification to the controller') the Board encourages to rephrase the sentence "*If and to the extent that it is not possible to provide the information at ones [once], it may be provided in stages without undue delay*" to make it clear that still all necessary information must be given, albeit at a later stage.

34. In Section 7.2.b ('Risk management procedure') the Board encourages to add references to Section 7.3 ('DPIA and prior consultation') to cover also the cases where the risks analysis and evaluation conclude that the processing would still result in a high residual risk. In addition, with regards to the last sentence of Section 7.2.b, the Board recommends to clarify that the procedure shall ensure that risk analyses, risk treatment plans and residual risks are clearly approved by the appropriate management.

35. While Section 8.7 ('International transfer of personal data (where applicable)') includes a comprehensive list of transfer tools available for third country transfers, the procedural aspect of that section is missing. The Board therefore recommends to add provisions on how to specifically meet the objective that the applicant demonstrably ensures GDPR compliance in that respect.

36. The Board notes that in Section 8.7.c ('Consulting the supervisory authority concerned') the reference to EDPB Recommendation 2/2020 is quite general and thus encourages to clarify the conditions in which a prior authorisation from the relevant supervisory authority is needed.

2.6 RIGHTS OF DATA SUBJECTS

37. Section 8.2.2 ('Providing information to the data subject') refers to the exemptions of the information obligation in Article 14 (5)(b) GDPR. However, the Board notes that it is missing a reference to the fact that where providing information is impossible or would involve a disproportionate effort, the controller must, in such cases, take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available. Therefore, the Board recommends to include this reference in order to align Section 8.2.2 with Article 14 (5)(b) GDPR. Furthermore, the Board recommends to clearly differentiate between the exemptions of the information obligation stipulated in Article 13(4) and Article 14 (5)(b) GDPR.

38. Section 8.2.2.b ('Preparing information to the data subjects') refers to the fact that *"the information provided to the data subject shall […] be demonstrably agreed with (the representatives of) the data subjects"*. However, the Board notes that the GDPR does not require a data subject "to agree" to information provided in line with Article 13 or Article 14 GDPR. Therefore, the Board recommends to use a different wording in Section 8.2.2.b in order to avoid misunderstandings.

39. The Board notes that Section 8.4.1.d ('Securing personal data (where applicable)') seems to apply only where personal data is stored "*for a short period of time*". However, in the view of the Board, a controller must always ensure compliance with the rights stipulated in Chapter III of the GDPR and, for example, not purposefully delete personal data when receiving an access request. Therefore, the Board recommends to delete the requirement "*for a short period of time*".

40. Regarding the handling of the rights of data subjects, Section 8.4.1.e ('Handling of the rights of the data subjects') refers to *"[…] without undue delay and in no case later than 30 days"* as timeline. In this regard, the Board recommends to refer instead to *"[…] within one month of receipt of the request"*, as stipulated in Article 12 (3) GDPR.

41. Section 8.4.2.b ('Providing a copy') foresees that the organisation *"provides […] the data subject, upon lawful and executable request, with a copy in a permanent form of his or her personal data that was processed by the organization"*. In order to avoid misunderstandings and different interpretations of this provision the Board recommends to refer instead to the need for the organisation to *"[…] provide a copy of the personal data undergoing processing"*, as stipulated in Article 15 (3) GDPR.

42. Regarding the right to erasure, Section 8.4.4.a states that "*The organisation shall determine and document whether and under what conditions the right of erasure applies to the processing activities*". The Board encourages to include a reference to Article 17 (3) GDPR to also cover and appropriately document situations where the right to erasure does not apply.

43. The Board notes that Section 8.4.6 ('The right to data portability (where applicable)') refers to the obligation for the organisation to, *"[…] where technically feasible, transmit such data directly to the intended recipient"* is used at the beginning of this section. In this respect, the Board recommends to use the wording *"[…] to another controller without hindrance"*, as stipulated in Article 20 (1) GDPR, to clarify that "another controller" refers to the one indicated by the data subject, and to indicate that the personal data covered by the right to data portability also includes data generated by the observation of the data subject's activity.

44. Section 8.4.7 ('The right to object'), refers to the processing for *"[…] scientific or historical purposes"*. In this respect however, the Board recommends to use the wording *"[…] scientific or historical research purposes or statistical purposes"*, as stipulated in Article 21 (6) GDPR.

45. Regarding the title of Section 8.4.8 ('The right regarding automated decision-making'), the Board recommends to change it to ''*the right regarding automated individual decision-making, including profiling"*, in line with the title of Article 22 GDPR. In addition, the Board notes that the part on ''objective'' under the same section refers to the need for the organisation to ''*ensure that automated individual decision making, including profiling, is carried out carefully*''. As it may not be possible to assess its implementation in practice, the Board recommends deleting the word "carefully" from this paragraph.

46. According to Section 8.4.8.f ('Bias check'), the *"[…] organisation shall demonstrably perform systematic analyses, at least annually, to determine the accuracy of the decision-making process and the absence of bias (distortion of results), and shall adjust the process as necessary."* In the view of the Board, it is not entirely clear if Section 8.4.8.f considers the "absence of bias" as an aspect of data accuracy. In any case, in order to avoid misunderstandings, the Board encourages to include a reference to Recital 71 GDPR in Section 8.4.8.f, as data accuracy in the context of profiling and of Article 22 GDPR is addressed there.

47. Section 8.4.10 foresees that where *"[…] the organisation refuses to comply with a request, it shall provide evidence that the request is manifestly unfounded or excessive"*. In contradiction to Article 12(5) GDPR, Section 8.4.10 could be misunderstood that in cases where the controller charges a reasonable fee for handling a data subject request, there is no such demonstration obligation. Therefore, the Board recommends to make clear that the burden of demonstrating the manifestly unfounded or excessive character of the request applies to both scenarios mentioned in Article 12 (5) (a) and (b) GDPR.

48. Regarding Section 8.4.11, the Board recommends to clarify whether the "complaints procedure" refer to dispute resolution processes or to formal complaints pursuant to Article 77 (1) GDPR.

2.7 RISKS FOR THE RIGHTS AND FREEDOMS OF NATURAL PERSONS

49. Regarding Section 7.3a, the Board recommends to include a reference to the lists pursuant to Article 35 (4) and (5) GDPR, as published by the NL SA.

50. The last sentence of Section 7.3.2 states "[…] or if the organisation develops processing operations under its own direction, comply with the requirements of Section 7.3 itself." The EDPB notes that in cases where an alleged processor develops processing operations under its own direction, the processor would not be a processor but a controller and then Section 7.3.2 would not be applicable at all. Therefore, the Board recommends to delete the last sentence of Section 7.3.2.

2.8 TECHNICAL AND ORGANISATIONAL MEASURES GUARANTEEING PROTECTION

51. The Board considers that it is not clear to what extent the term ''controls'' referred to in Section 7.2 ('Risk management') differs from the notion of ''technical and organisational measures''. The Board encourages to clarify this point accordingly.

55. The board notes that Section 7.4 ('Data protection by design and by default') of the certification criteria addresses the obligations related to data protection by design and by default pursuant to article 25 GDPR and encourages to include a reference to the criteria on processors and sub-processors already in Section 8.2.5, by taking them into account when contracting with these parties and when regularly reviewing and assessing processors' operations.

56. Similarly, the Board encourages to emphasise that processors should seek to facilitate data protection by design and by default in order to support the controllers' ability to comply with Article 25 obligations.

57. Finally, Section 7.5.1 ('Competences'') refers to the need for the organisation to, ''*where appropriate, take steps to acquire the necessary competence and evaluate the effectiveness of the steps taken"*. In the Board's view, the need to ensure that the persons carrying out the data processing activities have the required competences should always be assessed and ensured. The Board therefore encourages to amend this criteria accordingly.

3 CONCLUSIONS / RECOMMENDATIONS

By way of conclusion, the EDPB considers that:

regarding the ''*general remarks*'' the Board recommends that the NL SA

1. ensures throughout the certification scheme, that each certification criterion is designed in such a way as to enable reproducible assessment by several certification bodies in a consistent manner
2. clarifies throughout the certification scheme, that the scope is a national certification;
3. deletes in the introductory part reference to ''*unless* [it] ''*can demonstrate that the exclusions have no impact on the organisations ability to comply with the GDPR and this Standard*'';
4. adjusts throughout the certification scheme the terminology used in the requirements to the one in the GDPR;
5. rectifies throughout the certification scheme the numbering of sections or some redirections to other sections that are inaccurate.

regarding the *"scope of the certification mechanism and target of evaluation (TOE)",* the Board recommends that the NL SA

1. removes in Section 4.2.a reference according to which ''*exclusion of implementation criteria shall be justified*'';
2. includes in the certification scheme specific criteria to take into account the specificities of sub-processing or, in the alternative, indicates, in the introductory part, that sub- processors cannot be certified under the certification scheme;
3. amends the introduction to further specify the scope by referring to ''controllers, processors, joint controllers [and, if applicable, sub-processors]'' as well as the ''type of product and services'' provided by them;
4. clarifies in Section 4.1 that the assessment of all data processing activities that would fall within the scope of the certification are to be defined at the early stage of the definition of the ToE;
5. clarifies in Section 4.3 that the decision on the determination of the scope of the certification and ToE lies on the certification body after being suggested and described by the applicant.

regarding the "*lawfulness of the processing"* the Board recommends that the NL SA

1. amends Section 6.1.2 to make clear that only one legal basis needs to be chosen and complied with from those listed in Article 6 GDPR.
2. amends Section 6.1.2 to include the requirement to demonstrate the applicability of the legal basis and its appropriateness, where relevant, considering the processing activities, depending on the nature, context, scope and purposes of the processing;
3. adds a requirement in relation to children's consent in Section 6.1.2.b;
4. refers expressly to the conditions set out in Article 9 and 10 GDPR in Section 6.1.2.h.

regarding the "*principles of Article 5*" the Board recommends that the NL SA

1. clarifies in Section 6.1.1 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

2. adds in Section 6.1.1.c, point 3 (i), (ii) and (iii) a specific criterion according to which 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 Section 6.1.1.c point 3 (i), (ii) and (iii);
3. clarifies in Section 6.4.1 that data minimisation principle requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum;
4. clarifies in Section 6.1.4.b the requirement of *« longer period of time »* in order to allow for objective assessment by the applicant of its compliance with this criteria;
5. includes in Section 6.1.5 the obligation for the organisation to ensure deletion by processors to whom data has been shared or transmitted in accordance with Article 28(3)(g) GDPR;
6. deletes in Section 6.1.5 the reference that *''the retention period [...] may be indefinite''.*

regarding the "*general obligations for controllers and processors"* the Board recommends that the NL SA

1. deletes "where possible" in Section 6.2.a;
2. defines the requirements to be met regarding the arrangement concluded between the applicant and the other joint controllers involved in the ToE with regards to their respective responsibilities for compliance with the Brand Compliance certification criteria;
3. includes in Section 6.4.1.b criteria implementing the provisions of Article 26 (3) GDPR;
4. clarify in Section 7.2.b that the procedure shall ensure that risk analyses, risk treatment plans and residual risks are clearly approved by the appropriate management
5. includes in Section 8.7 provisions on how to specifically meet the objective that the applicant demonstrably ensures GDPR compliance in respect of data transfers;

regarding the *"rights of data subjects"* the Board recommends that the NL SA

1. includes in Section 8.2.2 a reference to the fact that where providing information is impossible or would involve a disproportionate effort, the controller must, in such cases, take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;
2. makes a clear distinction in Section 8.2.2 between the exemptions of the information obligation stipulated in Article 13(4) and Article 14 (5)(b) GDPR;
3. amend Section 8.2.2.b to make clear that the GDPR does not require a data subject "to agree" to information provided in line with Article 13 or Article 14 GDPR;
4. deletes in Section 8.4.1.d the reference to "*for a short period of time*";
5. refers in Section 8.4.1.e to *"[…] within one month of receipt of the request"*, as stipulated in Article 12 (3) GDPR;
6. refers in Section 8.4.2.b to the need for the organisation to *"[…] provide a copy of the personal data undergoing processing"*, as stipulated in Article 15 (3) GDPR;
7. uses in Section 8.4.6 the wording *"[…] to another controller without hindrance"*, as stipulated in Article 20 (1) GDPR to clarify that "another controller" refers to the one indicated by the data subject, and to indicate that the personal data covered by the right to data portability also includes data generated by the observation of the data subject's activity;
8. uses in Section 8.4.7 the wording *"[…] scientific or historical research purposes or statistical purposes"*, as stipulated in Article 21 (6) GDPR;
9. amends the title of Section 8.4.8 to refer to *''the right regarding automated individual decision-making, including profiling"*, in line with the title of Article 22 GDPR;

10. deletes in Section 8.4.8 reference to the term ''carefully'';
11. makes clear in Section 8.4.10 that the burden of demonstrating the manifestly unfounded or excessive character of the request applies for both scenarios mentioned in Article 12 (5) (a) and (b) GDPR;
12. clarifies in Section 8.4.11 whether the "complaints procedure" refer to dispute resolution processes or to formal complaints pursuant to Article 77 (1) GDPR.

regarding the "*risks for the rights and freedoms of natural persons*" the Board recommends that the NL SA

1. includes in Section 7.3a a reference to the lists pursuant to Article 35 (4) and (5) GDPR, as published by the Supervisory Authority of the Netherlands;
2. deletes the last sentence of Section 7.3.2.

Finally, in line with the Guidelines the EDPB also recalls that, in case of amendments of the Brand Compliance certification criteria involving substantial changes[7], the NL 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

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

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

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

The EDPB recalls that, pursuant to Article 43(6) of the GDPR, the NL SA 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

(Anu Talus)

[7] 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.