Opinion 27/2024 on the Brand Compliance criteria of certification regarding their approval by the Board as European Data Protection Seal pursuant to Article 42.5 (GDPR)

Adopted on 2 December 2024

Table of contents

The European Data Protection Board

Having regard to Article 63, Article 64(2) 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 Articles 10 and 22 of its Rules of Procedure.

(1) Member States, supervisory authorities, the European Data Protection Board (hereinafter "the EDPB or the Board") 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 certification mechanisms can enhance transparency and allow data subjects to assess the level of data protection of relevant products and services.[3]

(2) The criteria of certification form an integral part of a certification mechanism. Consequently, the GDPR requires the approval of the criteria of a national 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 propose the approval by the EDPB of a European data protection seal pursuant to article 42(5) of the GDPR, the SA should state the intention of the scheme owner to offer the certification mechanism in all Member States. In this case, 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(2) of the GDPR, the EDPB is approving the criteria of certification.

(4) This Opinion aims to ensure the consistent application of the GDPR, including by the SAs, controllers and processors in the light of the core elements, which certification mechanisms have to develop. In particular, the EDPB assessment is carried out on the basis "Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation" (hereinafter the "Guidelines") and their Addendum providing "Guidance on certification criteria assessment" (hereinafter the "Addendum").

(5) Accordingly, the EDPB acknowledges that each certification mechanism should be addressed individually and is without prejudice to the assessment of any other certification mechanism.

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

(6) Certification mechanisms should enable controllers and processors to demonstrate compliance with the GDPR. Therefore, its 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, scheme owner should ensure the alignment and conformity of the certification mechanism with any included or leveraged ISO standards and certification practices.

(8) As a result, certifications should add value to controllers and processors by helping to implement standardized and specified organizational and technical measures that demonstrably facilitate and enhance processing operation compliance to the GDPR, 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 supervisory authorities from exercising their tasks and powers pursuant to the GDPR and the relevant national laws.

(11) In this Opinion, the EDPB addresses issues, such as the scope of the criteria, the applicability and relevance of the criteria in all Member States.

(12) This 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 criteria in the context of its Opinion thereof, the latter does not encompass any kind of approval of such evaluation methods.

(13) The Opinion of the EDPB shall be adopted, pursuant to Article 64(2) 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 supervisory authority 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. If the opinion of the EDPB concludes that the criteria cannot be approved at stake, the SA may resubmit the criteria for approval when the concerns expressed in the initial EDPB Opinion are addressed.

HAS ADOPTED THE FOLLOWING OPINION:

SUMMARY OF THE FACTS

1. In accordance with Article 42(5) GDPR and the Guidelines, the draft “GDPR Certification Standard and Criteria, BC 5701:2024, Version 0.7” (hereinafter the “draft certification criteria”, “certification criteria” or “criteria”) was drafted by Brand Compliance B.V., a legal entity in the Netherlands (hereinafter the “scheme owner”), and submitted to Autoriteit Persoonsgegevens, the competent Supervisory Authority of the Netherlands (hereinafter the “NL SA’’).

2. The NL SA has submitted the draft certification criteria to the EDPB for approval pursuant to Article 64 (2) of the GDPR on 26 September 2024. The decision on the completeness of the file was taken on 12 November 2024.

3. The Brand Compliance certification mechanism 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

4. The EDPB has conducted its assessment of the criteria of certification for their approval under Articles 42(5) of the GDPR in line with the structure foreseen in Annex 2 to the Guidelines (hereinafter "Annex") and its Addendum.

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

5. The Brand Compliance certification mechanism contains certification criteria for the certification of processing operations performed on personal data by controllers or processors established in the European Union (EU) or in the European Economic Area (EEA).

6. The main criteria of this certification mechanism are divided into six sets of requirements, namely: Context of the data processing, including compliance with relevant EU or Member State law (set 1), Organisational framework conditions (set 2), Fundamentals of the processing activities, including the principles relating to the processing of personal data (set 3), Technical and organisational protection (set 4), Operational execution, including data subject rights (set 5), and Management system (set 6).

7. Certification applicants under this scheme must be controllers or processors. This includes processors who are directly entrusted with the processing of personal data by a controller within the meaning of Article 4(7) GDPR as well as sub-processors. Processing operations carried out (in part) as sub-processing will be certified in the organisational capacity of a processor.

8. The Board notes that the certification mechanism cannot be used to certify processing operations where two or more controllers jointly determine the purposes and means pursuant to Article 26(1) GDPR (joint controllers). The certification mechanism cannot be used to certify processing operations by an organisation located outside the EU or the EEA. Moreover, the certification mechanism cannot be used as transfer tool within the meaning of Article 42(2) and Article 46(2)(f) GDPR.

2.2 Processing operations

9. The certification mechanism can be applied to the processing of personal data regardless of the type and size of the organisation and regardless of the nature of the products or services it provides. Therefore, the scope of the certification mechanism is not limited to certain types of processing operations and allows for certification of any processing operations by a controller or processor. Hence, it is of fundamental importance that the methodological requirements are adhered to, as this is the only way to ensure a uniform application of the certification criteria and a comparable level of testing across different certification procedures. The aim is to ensure comparability and reproducibility of the certifications issued and their results.

2.3 Lawfulness of processing

10. The criteria require the examination of whether the processing operations of a controller comply with the provisions of Article 6 (section 6.1.2 of the criteria) and, where applicable, Article 9 (section 6.1.2.h of the criteria) as well as Article 10 GDPR (section 6.1.2.i of the criteria). Although compliance with the principle of lawfulness of the processing is an obligation of the controller, a processor must still adhere to specific requirements in this context (section 6.2 of the criteria). These requirements are particularly aimed at ensuring that the authorization for data processing is legitimately derived from the controller and that the processor supports the controller in complying with the GDPR, including the principle of lawfulness.

2.4 Principles of data processing

11. The criteria establish specific requirements for the assessment of all principles relating to the processing of personal data within the meaning of Article 5 GDPR (section 6 of the criteria). Insofar as the requirements for processors are concerned, separate criteria must be assessed in this context (section 6.2 of the criteria). As previously mentioned, the primary focus of the requirements for processors is to support the controller in implementing compliance with the principles.

2.5 General obligations of controllers and processors

12. The criteria reflect on the relationship between controllers and processors. In particular, the criteria establish the obligation for controllers and processors to comply with the requirements related to the outsourcing of processing activities, which includes, among other things, adherence to the provisions of Article 28(3) GDPR (section 8.5 of the criteria). Where processors are concerned, they must also comply with the specific requirements for processing under the authority of a controller (section 8.6 of the criteria). Additionally, further requirements are established to take into account the circumstances of sub-processing (section 6.2.e and in particular section 8.6.g of the criteria).

13. The criteria check the content of the records of processing activities in accordance with Article 30 GDPR (section 5.4 of the criteria). In this context, a distinction is made between the required content of a record of processing activities for controllers and processors in line with Article 30 (1) and (2) GDPR.

14. The criteria require applicants to appoint a Data Protection Officer (DPO) in accordance with Article 37 GDPR. Furthermore, the criteria ensure that the requirements under Articles 37 to 39 GDPR are fulfilled (section 5.3.2 of the criteria).

15. In relation to the principle of accountability pursuant to Article 5(2) and Article 24 GDPR, requirements are established for the organisation of data protection and reporting mechanisms (section 5.1 and 5.3 of the criteria), as well as the implementation of data protection policies (section 5.2 of the criteria).

2.6 Rights of the data subjects

16. The criteria provide adequate requirements for data subject rights in accordance with Chapter III of the GDPR. First, the requirements for transparent information, communication and modalities for the exercise of the rights of data subjects are addressed, followed by a detailed examination of the

respective data subject rights (section 8.4 of the criteria). Insofar as the requirements for processors are concerned, specific provisions for assistance obligations are set out (section 8.4.11 of the criteria)

2.7 Risks for the rights and freedom

17. The criteria require the controller to be aware of the possible risks to the rights and freedoms of natural persons for the data processing involved in the ToE. If the processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons, several criteria ensure that the applicant demonstrates that the requirements of Article 35 GDPR are fulfilled (section 7.3 of the criteria). Additionally, specific requirements for the assistance obligations of processors under Article 35 of the GDPR are also stipulated.

2.8 Technical and organisational measures guaranteeing protection

18. The criteria require the application of technical and organisational measures based on an information security standard providing confidentiality, integrity and accuracy of the personal data processed and the resilience the processing system. The criteria also require the application of measures to implement data protection by design and by default in accordance with Article 25 GDPR (section 7.4 of the criteria). The criteria establish specific requirements for controllers regarding the assessment of the notification of a personal data breach to the supervisory authority and, where necessary, the communication of such a personal data breach to the data subject in accordance with Articles 33 and 34 GDPR (section 8.8 of the criteria). In this context, specific obligations for processors are also outlined, particularly regarding the identification of a personal data breach and communication with the controller (sections 8.8.1 and 8.8.4 of the criteria).

2.9 Criteria for the purpose of demonstrating the existence of appropriate safeguards for transfer of personal data

19. The criteria require identifying all personal data transfers to third countries and to international organizations involved in the ToE and substantiating the choice made regarding the data transfer mechanism providing for appropriate safeguards, pursuant to Chapter V GDPR (section 8.7 of the criteria). The criteria provide a procedure for assessing of the intended transfers, such as monitoring its lawfulness.

3. ADDITIONAL CRITERIA FOR A EUROPEAN DATA PROTECTION SEAL

20. According to the Guidelines, the assessment shall include the question on “whether the criteria are able to take into account Member State data protection laws or scenarios”. Section 4.3 of the criteria requires the applicant to comply with applicable national and relevant sector-specific data protection law. The organisation shall correctly and comprehensively identify, analyse and document the relevant Member State or sector-specific laws and regulations applicable to the processing of personal data within the ToE. The documentation shall identify the person(s) responsible for drafting the national or sector-specific legal framework that is relevant for the ToE and their legal expertise. Furthermore, the Board understands that the appropriateness of the identification and elaboration of that legal framework is determined by the certifying body.

CONCLUSIONS / RECOMMENDATIONS

21. By way of conclusion, the EDPB considers that the Brand Compliance criteria of certification are consistent with the GDPR and approves them pursuant to the task of the Board defined in Article 70(1)(o) of the GDPR, resulting in a common certification (European Data Protection Seal).

22. The EDPB will register the "GDPR Certification Standard and Criteria, BC 5701:2024, Version 0.7" certification mechanism in the public register of certification mechanisms and data protection seals and marks pursuant to Article 42(8).

FINAL REMARKS

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

For the European Data Protection Board

The Chair
Anu Talus