Opinion 3/2025 on the draft decision of the French Supervisory Authority (FR SA) regarding the “Lexing GDPR certification criteria”

Adopted on 8 April 2025

Table of contents

The European Data Protection Board

Having regard to Article 63, Article 64(1)(c) and Article 42 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the European Economic Area (hereinafter "EEA") Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Article 64(1)(c) of the GDPR and Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) Member States, supervisory authorities, the European Data Protection Board (hereinafter "the EDPB") and the European Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms (hereinafter "certification mechanisms") and of data protection seals and marks, for the purpose of demonstrating compliance with the GDPR of processing operations by controllers and processors, taking into account the specific needs of micro, small and medium-sized enterprises[2]. In addition, the establishment of certifications can enhance transparency and allow data subjects to assess the level of data protection of relevant products and services[3].
(2) The certification criteria form an integral part of any certification mechanism. Consequently, the GDPR requires the approval of national certification criteria of a certification mechanism by the competent supervisory authority (Articles 42(5) and 43(2)(b) of the GDPR), or in the case of a European Data Protection Seal, by the EDPB (Articles 42(5) and 70(1)(o) of the GDPR).
(3) When a supervisory authority (hereinafter "SA") intends to approve a certification pursuant to Article 42(5) of the GDPR, the main role of the EDPB is to ensure the consistent application of the GDPR, through the consistency mechanism referred to in Articles 63, 64 and 65 of the GDPR. In this framework, according to Article 64(1)(c) of the GDPR, the EDPB is required to issue an Opinion on the SA's draft decision approving the certification criteria.
(4) This Opinion aims to ensure the consistent application of the GDPR, including by the SAs, controllers and processors in the light of the core elements which certification mechanisms have to develop. In particular, the EDPB assessment is carried out on the basis "Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation" (hereinafter the "Guidelines") and their Addendum providing "Guidance on certification criteria assessment" (hereinafter the "Addendum").
(5) Accordingly, the EDPB acknowledges that each certification mechanism should be addressed individually and is without prejudice to the assessment of any other certification mechanism.

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

(6) Certification mechanisms should enable controllers and processors to demonstrate compliance with the GDPR; therefore, the certification criteria should properly reflect the requirements and principles concerning the protection of personal data laid down in the GDPR and contribute to its consistent application.

(7) At the same time, the certification criteria should take into account and, where appropriate, be inter-operable with other standards, such as ISO standards, and certification practices.

(8) As a result, certifications should add value to an organisation by helping to implement standardized and specified organisational and technical measures that demonstrably facilitate and enhance processing operation compliance, taking account of sector-specific requirements.

(9) The EDPB welcomes the efforts made by scheme owners to elaborate certification mechanisms, which are practical and potentially cost-effective tools to ensure greater consistency with the GDPR and foster the right to privacy and data protection of data subjects by increasing transparency.

(10) The EDPB recalls that certifications are voluntary accountability tools, and that the adherence to a certification mechanism does not reduce the responsibility of controllers or processors for compliance with the GDPR or prevent SAs from exercising their tasks and powers pursuant to the GDPR and the relevant national laws.

(11) The Opinion of the EDPB shall be adopted, pursuant to Article 64(1)(c) of GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks from the first working day after the Chair and the competent SA have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

(12) The EDPB 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) GDPR and the Guidelines, the “Lexing GDPR certification criteria” (hereinafter the “draft certification criteria” or “certification criteria”) were drafted by Lexing, a legal entity registered in France (RCS PARIS 452 160 856) and submitted to the French Supervisory Authority (hereinafter the “FR SA”).

2. The FR SA has submitted its draft decision approving the certification criteria, and requested an Opinion of the EDPB pursuant to Article 64(1)(c) GDPR on 30 January 2025. The decision on the completeness of the file was taken on 26 February 2025.

3. The present certification is not a certification according to article 46(2)(f) 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 adhered to.

2 ASSESSMENT

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

2.1 GENERAL REMARKS

5. Under draft criterion R05-S01-C01 the scheme introduces a classification of types of personal data into five categories. The EDPB observes that although such a classification may indeed facilitate the overall risk assessment[4], a proper assessment should also take other factors apart from the types of personal data, such as the nature, scope, context and purposes of the processing, into consideration.

6. The Board welcomes the inclusion of section 1 on "Requirements relating to General Management's commitments in the field of data protection" in the draft certification criteria. The Board notes that draft criterion R01-S01-C01 on orientation for the application of data protection law provides that "if substantial orientations are updated, a new communication shall be sent before the end of the three-year period within one month of the update". In this context, the Board notes that the term "substantial" can be quite broad, can lead to ambiguity and can hinder the auditability of this criterion. To this purpose, the Board encourages the FR SA to require the scheme owner to further elaborate on which orientations are "substantial" (e.g. by providing some examples thereof).

7. The Board takes note of the approach taken and described under "1. Overview" in the certification criteria. The Board also notes that some criteria refer to the relevant GDPR provisions to which they aim at demonstrating compliance[5], and that Annex 5 consists of a "Concordance table between GDPR obligations and scheme criteria". However, references to the applicable GDPR provisions within the criteria are not systematic, and Annex 5 is not exhaustive[6]. The Board recalls that under "General requirements", Annex 2 of the Guidelines 1/2018 prescribes that all normative references are identified. Therefore, the Boards recommends the FR SA to require the scheme owner to make Annex 5 more granular by providing further details on the correspondence between the provisions of the GDPR and the certification criteria, to easily identify which criteria

[4] See Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in high risk" for the purposes of Regulation 2016/679 on 4 April 2017, WP 248 rev.1 endorsed by the EDPB on 25 May 2018, pp.9-10.
[5] For example, under the "Requirements relating to personal data protection by design" (R10), page 49 of the certification criteria, there is a reference to Article 25(1) GDPR in footnote 85.
[6] For example, under "requirements relating to the rights of data subjects (R15)" there is no reference to Article 12 GDPR and the latter also does not appear in Annex 5 as far as the "Requirements relating to the rights of data subjects" are concerned.

enables an applicant to demonstrate compliance with the GDPR. Alternatively, the Board recommends the FR SA to require the scheme owner to make a reference to the relevant GDPR provision for each criterion throughout the entire document of the certification criteria.

8. The Board notes that the scheme owner defines the term "anonymisation"[7] in annex 4 of the certification criteria. Taking into account that the notion of anonymisation is not explicitly defined in the GDPR, the EDPB encourages the competent SA to require the scheme owner to consider whether having such a definition is necessary. If a definition of "anonymisation" is considered necessary, the EDPB recommends the competent SA to require the scheme owner to ensure that the term is defined in accordance with recital 26 GDPR[8].

2.2 LEGAL BASIS - CONSENT

9. Regarding the consent of children, the Board notes that in draft criterion R06-S03-C02 on "Specific conditions for consent" states that "When considering choosing consent as a legal basis, the applicant [...] shall also ensure where the data subject is a minor below the age of 16 years, that consent is given or authorised by the holder of parental responsibility". The Board notes that according to Article 8(1) GDPR the national laws of the member states can establish different age limits. However, the Board could not identify any reference in the criteria to the national law that provides for a lower age limit where Article 6(1)(a) GDPR applies, in relation to the offer of information society services directly to a child, in line with Article 8(1) GDPR. Therefore, the Board recommends that the FR SA requires the scheme owner to modify this criterion accordingly.

10. Furthermore, concerning draft criterion R06-S03-C02, the Board also understands that the certification body will always conduct an assessment of the documented results of the verification carried out, to ensure that the specific conditions for consent have been met pursuant to Article 7 GDPR. In this respect, the Board recommends the competent SA to require the scheme owner to also cover the requirements stemming from Article 8(2) GDPR.

2.3 PRINCIPLES OF ARTICLE 5

11. The Board welcomes section 5.3 of the draft criteria and in particular criterion R05-S03-C01 on the principles of fairness and transparency, as well as relevant policies. The Board notes that while for the principle of transparency there are detailed criteria, for the fairness principle this is not the case. In this context, The Board reiterates that the certification criteria shall be a stand-alone document, where all the criteria are sufficiently and specifically elaborated to be auditable. In this regard, the Board notes that within its Guidelines 04/2019 on Article 25 GDPR Data Protection by Design and by

[7] See page. 108, "A process that ensures that data can no longer be used to identify the individual to whom it relates, that separate data relating to the same individual cannot be linked, and that no information about an individual can be deduced".
[8] The also EDPB highlights that the definition may require adaptation following further guidance from the EDPB or jurisprudence from the CJEU.

Default (adopted on 20 October 2020), the Board lists several elements that should be taken into account in order to comply with the principle of fairness. Therefore, for completeness and auditability of the criteria, the Board recommends the FR SA to require the scheme owner to further develop specific, precise and auditable criteria, in so far that they are not already covered in other parts of the criteria, based on all the elements listed in the EDPB Guidelines 4/2019 on Article 25 GDPR regarding Data Protection by Design and by Default, paragraph 70[9].

12. In chapter 5.4 S04 on "Requirements relating to purposes", the scheme defines the requirements for the principle of purpose limitation and criterion R05-S04-C01 prohibits further processing of personal data for purposes that are incompatible with the specified, explicit and legitimate purposes for which the data were initially collected. However, the provisions of Article 6(4) GDPR on the compatibility check for further processing are not fully reflected in the criteria. Therefore, the Board recommends the competent SA to require the scheme owner to further develop specific certification criteria on in order to fully cover the requirements of Article 6(4) GDPR.

2.3. GENERAL OBLIGATIONS FOR CONTROLLERS

2.3.1. Obligations applicable to the controllers

13. With respect to section 1.2 on "Requirements relating to personal data protection policies" the Board welcomes the list of information to be provided to the data subjects. However, the Board notes that the draft certification criteria, do not include a reference to Article 13(3) GDPR, which states that "*where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in* [*Article 13(2)*]". For the sake of completeness of the criteria in this section, the Board recommends the FR SA to require the scheme owner to revise the criteria in order to cover the requirements of Article 13(3) GDPR.

14. The Board notes that the draft certification criteria require that the applicants should appoint a DPO. The EDPB also welcomes the fact that the draft certification criteria requires the DPO to report directly to the highest management level, according to draft criterion R02-S04-C01, which is in line with Article 38(3) GDPR, and that the applicant shall establish a network of DPO intermediaries according to draft criterion R03-S01-C03. In the view of the Board, DPOs can indeed perform their tasks better if they interact with employees at all hierarchical levels within the applicant's structure. However, the EDPB encourages the competent SA to require the scheme owner to include a definition of the term "intermediaries", including explanations about their role vis-a-vis the DPO.

15. Moreover, the draft criterion R02-S05-C01 requires that the applicant provide the DPO with a dedicated budget each year to perform his or her tasks. However, Article 38(2) GDPR states that: "The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry *out those tasks and access to personal data and processing operations, and to maintain*

[9] See EDPB Opinion 18/2024 on the draft decision of the Austrian Supervisory Authority regarding DSGVO-zt GmbH certification criteria, adopted on 16 July 2024, paragraph 22.

his or her expert knowledge", meaning that it refers to the more general term "resources", which also includes time, training and equipment. For that reason, the EDPB recommends the FR SA to require the scheme owner to adapt the criteria, to the effect that the resources allocated to the DPO do not only cover performance of tasks, but also maintenance of knowledge, in line with Article 38(2) GDPR.

2.4 RIGHTS OF DATA SUBJECTS

16. The Board notes that under draft criterion R15-S02-C03, regarding "Response time"[10], to requests to exercise data subjects' rights "*the applicant shall respond to requests to exercise rights within one month of receipt of the request*". The Board notes that the draft criterion does not refer to the relevant provisions under Article 12 GDPR and highlights that pursuant to Article 12(3) GDPR, a controller shall provide information on action taken on a request under Articles 15 to 22 "*without undue delay*"[11]. Therefore, the Board recommends the FR SA to require the scheme owner to adapt the relevant criteria, to ensure that applicants provide information on action taken without undue delay and at latest within one month of receipt of the request.

17. The Board notes that Article 13(2)(c) GDPR requires that the information to be provided to data subjects includes the right to withdraw consent, when relevant. In this regard the Board notes that this possibility is not mentioned in draft criteria R01-S02-C04, R01-S02-C08 and R01-S02-C11. Therefore, the Board recommends the FR SA to require the scheme owner to modify these criteria accordingly so that this requirement is also reflected in the applicants' policies.

2.5 RISKS FOR THE RIGHTS AND FREEDOMS OF NATURAL PERSONS AND TECHNICAL AND ORGANISATIONAL MEASURES GUARANTEEING PROTECTION

18. According to article 25(1) GDPR the obligation of data protection by design applies "*both at the time of the determination of the means for processing and at the time of the processing itself*". However, the Board notes that the wording of draft criterion R10-S02-C01 creates the impression that it is only the processing operations set up in the last two years that are subject to compliance with the obligation of data protection by design. In this regard, the EDPB recommends the competent SA to require the scheme owner to rephrase the relevant passage in a way that clarifies that certification requires the evaluation of all the processing operations within the scope of the ToE in relation to the obligation of data protection by design, regardless of when the processing operations were initiated.

19. The EDPB welcomes that draft criterion R10-S02-C03 requires applicants to carry out an annual audit in compliance with draft criterion R01-S03-C04, to ensure that the procedure for data protection by design is applied. However, the EDPB considers that

[10] Part of the "15. Requirements relating to the rights of data subjects (R15)".
[11] See also Recital 59 GDPR.

this requirement should be complemented by procedures which ensure that adjustments can be made continuously to individual measures adopted by applicants, to ensure data protection design in compliance with Article 25(1) GDPR[12]. Therefore, the EDPB recommends the FR SA to require the scheme owner to adjust the criteria in section 10.2 (for example in draft criterion R10-S02-C02) to the effect that the criteria require applicants to implement procedures for continuous adjustment of measures adopted for compliance with Article 25(1) GDPR.

20. In draft criteria R13-S03 and R13-S05, the certification scheme refers to the necessary measures that the applicant should implement to mitigate the risks identified in the data protection impact assessment (DPIA). The Board notes that the scheme uses the term "corrective measures" in that respect. This terminological choice is unclear as the term "corrective" refers to the powers of the DPAs, in Article 58(2) GDPR. Therefore, the EDPB encourages the competent SA to require the scheme owner to clarify that the term "corrective measures" does not refer to the corrective powers of the DPAs, but to mitigating measures in relation to non-conformity.

2.6 TECHNICAL AND ORGANISATIONAL MEASURES GUARANTEEING PROTECTION

21. The Board notes that draft criterion R14-S09-C02 on "Software development procedure – content", refers to the content of the procedure relating to software developments. The Board also notes that draft criterion R14-S17-C02 includes a procedure for back-up. For the completeness of criterion R14-S09-C02, the Board considers it important to also include a backup procedure. Therefore, the Board encourages the competent SA to require the scheme owner to include a process for back-up before any upgrade or deployment of software.

22. Regarding draft criterion R14-S19-C05, "Network activity monitoring", the Board welcomes the inclusion of the statement that "*the applicant shall have software enabling it to analyse activity on its network under the conditions referred to in criterion R14-S18-C06*". However, taking into account that the draft criteria require that the applicant establishes a procedure for each processing activity, the Board recommends the competent SA to require the scheme owner to modify this criterion, to also require that the applicant shall set up a network activity monitoring procedure allowing the activity on its network to be analysed under the conditions referred to in draft criterion R14-S18-C06.

3 CONCLUSIONS / RECOMMENDATIONS

By way of conclusion, the EDPB considers that

23. regarding the "general remarks", the Board recommends that the FR SA:

1. require the scheme owner to make Annex 5 more granular by providing further details on the correspondence between the provisions of the GDPR and the certification

[12] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, adopted on 13 November 2019 and adopted after public consultation on 20 October 2020, paragraph. 3.

criteria, to easily identify which criteria enables an applicant to demonstrate compliance with the GDPR. Alternatively, the Board recommends the FR SA to require the scheme owner to make a reference to the relevant GDPR provision for each criterion throughout the entire document of the certification criteria.

2. require the scheme owner, if a definition of the term "anonymisation" is necessary, to ensure that the term is defined in accordance with recital 26 GDPR.

24. regarding the "legal basis - consent" the Board recommends that the FR SA:

1. require the scheme owner to refer, in the criterion R06-S03-C02 to the national law that provides for a lower age limit where Article 6(1)(a) GDPR applies, in relation to the offer of information society services directly to a child, in line with Article 8(1) GDPR.

2. require the scheme owner, with respect to the criterion R06-S03-C02 to also cover the requirements stemming from Article 8(2) GDPR.

25. regarding the "principles of Article 5" the Board recommends that the FR SA:

1. require the scheme owner to further develop specific criteria in order to fully cover the provisions of Article 6(4) GDPR on the compatibility check for the further processing.

2. require the scheme owner to further develop specific, precise and auditable criteria, in so far that they are not already covered in other parts of the criteria, based on all the elements listed in the EDPB Guidelines 4/2019 on Article 25 GDPR regarding Data Protection by Design and by Default, paragraph 70.

26. regarding the "general obligations for controllers and processors" the Board recommends that the FR SA:

1. require the scheme owner to add to section 1.2. of the certification criteria the provision of the Article 13(3) GDPR, namely that that "*where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in* [*Article 13(2)*]" for the sake of completeness.

2. require the scheme owner to adapt the criterion R02-S05-C01 in order to clarify that the resources allocated to the DPO do not only cover performance of tasks, but also maintenance of knowledge, in line with Article 38(2) GDPR.

27. regarding the "rights of data subjects" the Board recommends that the FR SA:

1. require the scheme owner to adapt the criterion R15-S02-C03 , to ensure that applicants provide information on action taken without undue delay and at latest within one month of receipt of the request.

2. require the scheme owner to revise criteria R01-S02-C04, R01-S02-C08 and R01-S02-C11 in order to include the obligations of Article 13(2)(c) GDPR, which provides that the information to be provided to data subjects includes the right to withdraw consent, when relevant

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

1. require the scheme owner to rephrase the relevant passage of the criterion R10 S02-C01 in a way that clarifies that certification requires the evaluation of all the processing operations within the scope of the ToE in relation to the obligation of data protection by design, regardless of when the processing operations were initiated.

2. require the scheme owner to adjust the criteria in section 10.2 (for example in draft criterion R10-S02-C02) to the effect that the criteria require applicants to implement procedures for continuous adjustment of measures adopted for compliance with Article 25(1) GDPR.

3. require the scheme owner to modify criterion R14-S19-C05, to also require that the applicant shall set up a network activity monitoring procedure allowing the activity on its network to be analysed under the conditions referred to in draft criterion R14-S18-C06.

29. Finally, in line with the Guidelines the EDPB also recalls that, in case of amendments of the Lexing certification criteria involving substantial changes[13], the FR 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

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

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

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

33. The EDPB recalls that, pursuant to Article 43(6) of the GDPR, the FR SA shall make public the Lexing 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.

[13] 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.

For the European Data Protection Board
The Chair

(Anu Talus)