Opinion 15/2022 on the draft decision of the competent supervisory authority of Luxembourg regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR

Adopted on 4 July 2022

Table of contents

The European Data Protection Board

Having regard to Article 63, Article 64 (1)(c), (3)-(8) and Article 41 (3) 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 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 10 and Article 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the European Data Protection Board (hereinafter "the Board") is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter "SA") intends to approve the requirements for accreditation of a code of conduct (hereinafter "code") monitoring body pursuant to article 41. The aim of this opinion is therefore to contribute to a harmonised approach with regard to the suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a code monitoring body by the competent supervisory authority. Even though the GDPR does not directly impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinion by: firstly, requesting the competent SAs to draft their requirements for accreditation of monitoring bodies based on article 41(2) GDPR and on the Board's "Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679" (hereinafter the "Guidelines"), using the eight requirements as outlined in the guidelines' accreditation section (section 12); secondly, providing the competent SAs with written guidance explaining the accreditation requirements; and, finally, requesting the competent SAs to adopt the requirements in line with this opinion, so as to achieve an harmonised approach.

(2) With reference to article 41 GDPR, the competent supervisory authorities shall adopt requirements for accreditation of monitoring bodies of approved codes. They shall, however, apply the consistency mechanism in order to allow the setting of suitable requirements ensuring that monitoring bodies carry out the monitoring of compliance with codes in a competent, consistent and independent manner, thereby facilitating the proper implementation of codes across the Union and, as a result, contributing to the proper application of the GDPR.

(3) In order for a code covering non-public authorities and bodies to be approved, a monitoring body (or bodies) must be identified as part of the code and accredited by the competent SA as being capable of effectively monitoring the code. The GDPR does not define the term "accreditation". However, article 41 (2) of the GDPR outlines general requirements for the accreditation of the monitoring body. There are a number of requirements, which should be met in order to satisfy the competent supervisory authority to accredit a monitoring body. Code owners are required to explain and

[1] References to the "Union" made throughout this opinion should be understood as references to "EEA".

demonstrate how their proposed monitoring body meets the requirements set out in article 41 (2) GDPR to obtain accreditation.

(4) While the requirements for accreditation of monitoring bodies are subject to the consistency mechanism, the development of the accreditation requirements foreseen in the Guidelines should take into consideration the code's sector or specificities. Competent supervisory authorities have discretion with regard to the scope and specificities of each code, and should take into account their relevant legislation. The aim of the Board's opinion is therefore to avoid significant inconsistencies that may affect the performance of monitoring bodies and consequently the reputation of GDPR codes of conduct and their monitoring bodies.

(5) In this respect, the Guidelines adopted by the Board will serve as a guiding thread in the context of the consistency mechanism. Notably, in the Guidelines, the Board has clarified that even though the accreditation of a monitoring body applies only for a specific code, a monitoring body may be accredited for more than one code, provided it satisfies the requirements for accreditation for each code.

(6) The opinion of the Board shall be adopted pursuant to article 64 (3) 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.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The Luxembourg Supervisory Authority (hereinafter "LU SA") has submitted its draft decision containing the accreditation requirements for a code of conduct monitoring body to the Board, requesting its opinion pursuant to article 64 (1)(c), for a consistent approach at Union level. The decision on the completeness of the file was taken on 28 March 2022.

2 ASSESSMENT

2.1 General reasoning of the Board regarding the submitted draft accreditation requirements

2. All accreditation requirements submitted to the Board for an opinion must fully address article 41 (2) GDPR criteria and should be in line with the eight areas outlined by the Board in the accreditation section of the Guidelines (section 12, pages 21-25). The Board opinion aims at ensuring consistency and a correct application of article 41 (2) GDPR as regards the presented draft.

3. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to articles 41 (3) and 57 (1) (p) GDPR, all the SAs should cover these basic core requirements foreseen in the Guidelines, and the Board may recommend that the SAs amend their drafts accordingly to ensure consistency.

4. All codes covering non-public authorities and bodies are required to have accredited monitoring bodies. The GDPR expressly request SAs, the Board and the Commission to "encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium sized enterprises." (article 40 (1) GDPR). Therefore, the Board recognises that the requirements need to work for different types of codes, applying to sectors of diverse size, addressing various interests at stake and covering processing activities with different levels of risk.

5. In some areas, the Board will support the development of harmonised requirements by encouraging the SA to consider the examples provided for clarification purposes.

6. When this opinion remains silent on a specific requirement, it means that the Board is not asking the LU SA to take further action.

7. This opinion does not reflect upon items submitted by the LU SA, which are outside the scope of article 41 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

2.2 Analysis of the LU SA's accreditation requirements for Code of Conduct's monitoring bodies

8. Taking into account that:

   a. Article 41 (2) GDPR provides a list of accreditation areas that a monitoring body need to address in order to be accredited;
   b. Article 41 (4) GDPR requires that all codes (excluding those covering public authorities per Article 41 (6)) have an accredited monitoring body; and
   c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for monitoring bodies and conduct the accreditation of a body for monitoring codes of conduct.

the Board is of the opinion that:

2.2.1 GENERAL REMARKS

9. The Board notes that on 22 February 2022, "the Guidelines 04/2021 on Codes of Conduct as tools for transfers" were adopted. These guidelines do not add any additional requirements for the accreditation of monitoring bodies that monitor codes of conduct intended for international transfers. Rather, the guidelines provide further specifications of the general requirements established by the Guidelines 1/2019 (Section 12) taking into account the specific context of international transfers[2]. For the sake of clarity, the Board recommends the LU SA to add a reference to the above-mentioned guidelines, which are relevant in the context of monitoring codes of conduct intended for international transfers.

[2] See Section4.2 of the EDPB Guidelines 04/2021 on Codes of Conduct as tools for transfers

10. The Board encourages the LU SA to include either in the draft accreditation requirements or in the complementary guidance to the requirements, some examples of the information or documents that applicants have to submit when applying for accreditation.

11. The Board notes that the requirements state that an internal monitoring body "could be an internal department within the code owner". The Board considers that it should be made explicit that an internal monitoring body cannot be setup within a code member. Therefore, the Board recommends adding a relevant provision.

12. The Board notes that there is no reference to the duration of the accreditation or accreditation withdrawal procedures. Whilst the Board accepts that these areas fall into the area of guidance supporting the accreditation requirements, the Board considers them important areas in terms of ensuring that the whole accreditation process is transparent. On the basis of the explanations provided by the LU SA, the Board understands that the information will be included in the accreditation procedure, and welcomes such inclusion.

13. The Board observes that the LU SA's draft accreditation requirements are sometimes worded in present tense, instead of as an obligation (e.g. sections 5.5 and 6.1). For the sake of clarity, the Board recommends that the LU SA formulate the requirements as an obligation (ie. using "shall", "must", or equivalent term).

14. The Board observes that the draft requirements make several references to "audit", instead of "monitoring". Based on the explanations provided by the LU SA, the Board understands that "audit" is used as a synonym of "monitoring". However, in order to avoid confusion, the Board encourages the LU SA to make it clearer.

2.2.2 INDEPENDENCE

15. The Board welcomes the inclusion of explanatory notes in the LU SA's draft accreditation requirements, as they contribute to improve the clarity and understanding thereof.

16. The Board considers that the requirements concerning the organisational and financial independence of the monitoring body (section 1.4 and 1.7 of the draft requirements, respectively) should address the boundary conditions that determine the concrete requirements. These include the expected number, size and complexity of the code members (as monitored entities), the nature and scope of their activities (which are the subject of the code) and the complexity or degree of risk(s) of the relevant processing operation(s). Therefore, the Board encourages the LU SA to redraft the requirements accordingly.

17. Moreover, with regard to the organisational resources (section 1.4), the Board observes that the draft accreditation requirements refer to "adequate resources and personnel to effectively perform its task". The Board encourages LU SA to redraft the relevant part of the requirements by adding a reference to "sufficient number of sufficiently qualified personnel" and including a reference to technical resources necessary for the effective performance of the monitoring body's task.

18. In addition, the Board considers that the requirements on financial resources would benefit from the inclusion of some examples with regard to the financial independence of the monitoring body, in order to highlight how the monitoring body can demonstrate that the means by which it obtains financial support should not adversely affect its independence (section 1.7). For instance, the monitoring body would not be considered financially independent if the rules governing its financial support allow a code member, who is under investigation by the monitoring body, to stop its financial contributions to

it, in order to avoid a potential sanction from the monitoring body. The Board encourages the LU SA to such clarification and provide examples of how the monitoring body can provide such evidence.

19. Regarding section 1.5 on internal monitoring bodies, the Board considers that the impartiality of the internal monitoring body shall be ensured not only towards the larger entity, but towards the overall group structure. The Board encourages the LU SA to make the necessary amendments.

20. In addition, the Board underlines that, according to point 65 of the Guidelines, where an internal monitoring body is proposed, there should be separate personnel and management, accountability and function from other areas of the organisation. The LU SA's draft accreditation requirements do not include a reference to a separate accountability and, therefore, the Board recommends to add such reference. Likewise, the Board recommends the LU SA to add a requirement to prove that the internal monitoring body has a specific separated budget that is able to manage independently.

2.2.3 CONFLICT OF INTEREST

21. As a general remark in this section, the Board is of the opinion that, for practical reasons, more detailed examples of cases where a conflict of interest could arise might be helpful. An example of a conflict of interest situation would be the case where personnel conducting audits or making decisions on behalf of a monitoring body had previously worked for the code owner, or for any of the organisations adhering to the code. Therefore, the Board encourages the LU SA to elaborate on the examples included in the explanatory note.

22. Furthermore, the Board observes that the LU SA accreditation requirements do not explicitly include the obligation of the monitoring body to refrain from any action that is incompatible with its tasks and duties (paragraph 68, page 23 of the Guidelines). Therefore, the Board recommends the LU SA to align the text with the Guidelines and include the above-mentioned obligation.

2.2.4 EXPERTISE

23. The EDPB welcomes the explanations provided in the explanatory note and encourages the LU SA to include some addition examples of documentation that demonstrates the necessary experience, such as data protection certifications and training certificates.

24. With regard to section 3.5, the Board notes that it distinguishes 3 types of personnel: auditors, "other technical experts", legal experts. However, it is unclear what is the difference between the three types of personnel. In addition, point b) seems to imply that auditors are technical personnel. The Board considers that this curtails the possibility for legal personnel to perform audits. Therefore, the Board recommends the LU SA to clarify the differences between the three roles and ensure consistency in the requirements, in order to not curtail the freedom of the code owner to define the type of expertise required for each role.

25. Furthermore, the EDPB considers that the requirements for the personnel are very specific and may curtail the freedom of the code owner to define the specific expertise requirements in the code of conduct. The Board encourages the LU SA to make the requirements less restrictive by including a more general reference that takes into account the different types of codes, such as "a relevant level of experience in accordance with the code itself".

26. In addition, the Board observes that the LU SA makes a distinction between legal and technical personnel. The Board encourages the LU SA to clarify that the technical requirements of the personnel will depend on whether it is necessary for the code at stake.

2.2.5 ESTABLISHED PROCEDURES AND STRUCTURES

27. With regard to section 4.5, the Board notes that the procedure to ensure the monitoring of the code of conduct will take into account the "number of code members". Since the number of code members may not be known at the moment the monitoring body applies for accreditation, the Board encourages the LU SA to refer to the expected number and size of the code members.

28. The Board notes that section 4.6 should include a reference to regular reporting, in line with paragraph 72 of the Guidelines, and encourages the LU SA to do so.

2.2.6 TRANSPARENT COMPLAINT HANDLING

29. With regard to section 5, the Board recommends the LU SA to include the obligation of the monitoring body to inform the code member, the code owner, the LU SA and where, required, all concerned SAs about the measures taken and its justification without undue delay, in line with paragraph 77 of the Guidelines.

30. Finally, regarding the provision of evidence of suitable corrective measures (section 5.3), the Board encourages the LU SA to amend the text, in order to establish the obligation of the monitoring body to provide evidence of suitable and, if necessary, immediate corrective measures.

2.2.7 COMMUNICATION WITH THE LU SA

31. The Board notes that section 6.2 refers to changes "to the basis of accreditation". Based on the explanations provided by the LU SA, the Board understands that it refers to changes having an impact on the compliance to the accreditation requirements. The Board encourages the LU SA to add such clarification.

2.2.8 REVIEW MECHANISMS

32. As stated in the LU SA's draft accreditation requirements (section 7.2), the monitoring body shall ensure that it has documented plans and procedures to review the operation of the code to ensure that the code remains relevant to the members. In this respect, the Board underlines that changes in the application and interpretation of the law and new technological developments should be taken into consideration. Therefore, the Board encourages the LU SA to reflect it in the text.

33. The Board notes that under section 7.2 of the requirements there is no reference to the fact that the updating of the code of conduct is the responsibility of the code owner. The Board is of the opinion that, in order to avoid confusion, a reference to the code owner should be made. Therefore, the Board encourages the LU SA to add that the monitoring body shall apply and implement updates, amendments, and/or extensions to the Code, as decided by the code owner.

34. In addition, the Board considers that the annual report on the operation of the code should be at the disposal of the LU SA, and encourages the LU SA to amend the draft accordingly.

2.2.9 LEGAL STATUS

35. The Board encourages the LU SA to replace the term "European Union" by "European Economic Area" in section 8.1.

36. Regarding section 9, the EDPB recommends the LU SA to add that, when subcontractors are used, the monitoring body shall ensure effective monitoring of the services provided by the contracting entities. Moreover, the Board underlines the need to specify requirements relating to the termination of the contract, in particular so as to ensure that the subcontractors fulfil their data protection obligations,

and encourages the LU SA to add such remark. Finally, the Board encourages the LU SA to to provide examples of when subcontracting is allowed and to delete the sentence related to subcontracting in "punctual circumstances".

3 CONCLUSIONS / RECOMMENDATIONS

37. The draft accreditation requirements of the Luxembourgish Supervisory Authority may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:

38. Regarding *general remarks* the Board recommends that the LU SA:

1. to add a reference to the Guidelines 04/2021, which are relevant in the context of monitoring codes of conduct intended for international transfers.

2. make explicit that an internal monitoring body cannot be setup within a code member.

3. formulate the requirements as an obligation.

39. Regarding *independence* the Board recommends that the LU SA:

1. include a reference to a separate accountability

2. add a requirement to prove that the internal monitoring body has a specific separated budget that is able to manage independently

40. Regarding *conflict of interest* the Board recommends that the LU SA:

1. align the text with the Guidelines and include the obligation of the monitoring body to refrain from any action that is incompatible with its tasks and duties

41. Regarding *expertise* the Board recommends that the LU SA:

1. clarify the differences between the three types of personnel and ensure consistency in the requirements, in order to not curtail the freedom of the code owner to define the type of expertise required for each role.

42. Regarding *transparent complaint handling* the Board recommends that the LU SA:

1. include the obligation of the monitoring body to inform the code member, the code owner, the LU SA and where, required, all concerned SAs about the measures taken and its justification without undue delay, in line with paragraph 77 of the Guidelines.

43. Regarding *legal status* the Board recommends that the LU SA:

1. add in section 9 that, when subcontractors are used, the monitoring body shall ensure effective monitoring of the services provided by the contracting entities

4 FINAL REMARKS

44. This opinion is addressed to the Luxembourgish supervisory authority and will be made public pursuant to Article 64 (5) (b) GDPR.

45. According to Article 64 (7) and (8) GDPR, the LU SA shall communicate 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.

46. The LU SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)