Luxembourgish accreditation requirements for a GDPR code of conduct monitoring body

Introduction

General

In accordance with Article 41 (1) of the General Data Protection Regulation 2016/679 of 26 April 2016 (GDPR) and the European Data Protection Board Guidelines 01/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 (hereinafter referred to as the EDPB Guidelines) and the European Data Protection Board Guidelines 04/2021 on Codes of Conducts as tools for transfers, national and transnational codes of conduct have to be monitored by a monitoring body that is accredited by the competent supervisory authority (hereinafter referred to as the CNPD). According to Article 41 (6) of the GDPR, and specified in the EDPB Guidelines, the requirement of an accredited monitoring body does not apply for processing carried out by public authorities and bodies.

The monitoring body can be either external or internal to the code owner. An internal monitoring body could be an internal department within the code owner. Article 41 (2) of the GDPR sets out a number of requirements which the proposed monitoring body must meet in order to gain accreditation. A monitoring body must:

- Demonstrate independence and expertise in relation to the subject matter of the code, pursuant to Article 41 (2) (a);
- Demonstrate established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation, as per Article 41 (2) (b);
- Demonstrate established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public, as per Article 41 (2) (c); and
- Demonstrate to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests, as per Article 41 (2) (d).

The EDPB Guidelines under Regulation 2016/679 provide important practical guidance and interpretative assistance in relation to the application of Article 41 (2) of the GDPR. The EDPB Guidelines categorise the accreditation requirements in Article 41 (2) into the following eight categories:

- Independence
- Conflict of interest
- Expertise
- Established procedures and structures
- Transparent complaints handling
- Communication with the competent supervisory authority
- Review Mechanisms
- Legal status

The requirements listed in this document are based on the requirements of Article 41 (2) of the GDPR and the requirements set out in section 12 of the EDPB Guidelines 01/2019 on Codes of Conduct and Monitoring Bodies and follow the structure of the Guidelines.

The requirement for the CNPD to submit the draft criteria for accreditation of a monitoring body to the EDPB is set out in Article 41 (3) of the GDPR, pursuant to the consistency mechanism referred to in Articles 63 and 64 (1) (c). According to Article 57 (1) (p), the CNPD must publish these criteria.

Application Requirements

Applicants must fulfil all the accreditation requirements set out in this document to become accredited by the CNPD.

The requirements shall apply to the monitoring body, regardless of whether it is an internal or external monitoring body, unless otherwise specified.

Accreditation as a monitoring body is only possible in relation to the subject matter of one or more specific codes of conduct pursuant to Article 41 (1) of the GDPR.

Applications for accreditation must be submitted in writing to the CNPD. The application shall contain proof of fulfilment of the requirements by submitting relevant documents, certificates etc. as set out in these requirements as well as in the application procedure.

The application of the accreditation requirements for monitoring bodies shall take into account the specificities of each sector's processing.

Requirements

1. Independence

Explanatory note: The requirements below set out what constitutes independence. Independence for a monitoring body can be understood as a series of formal rules and procedures for the appointment, terms of reference and operation of the monitoring body. These rules and procedures will allow the monitoring body to perform its monitoring tasks without influence from third parties, such as members of the code or the code owner. Monitoring bodies will be structured and managed to safeguard their independence and impartiality and will be required to demonstrate this to the CNPD in their submission.

1.1 The monitoring body shall demonstrate that it has defined and implemented policies, procedures and other organisational measures to provide ongoing assurance regarding the independence of the monitoring body from the code owner, the code members, the profession, industry or sector to which the code applies.

1.2 The monitoring body shall have all personnel that is involved in the activities of the monitoring body formally commit to impartiality.

1.3 The monitoring body shall take all decisions or sanctions related to monitoring activities independently without involving other bodies such as the code owner or code members. This could be evidenced by formal rules for appointment, terms of reference, powers and operation of any committees or personnel that may be involved with an internal monitoring body (such committees or personnel shall be free from any commercial, financial and other pressures that might influence decisions).

1.4 The monitoring body shall demonstrate that it has sufficient number of sufficiently qualified personnel to effectively perform its tasks, that it is able to act independently from code owners and code members and is protected from interference or sanctions as a result of this duty. The qualified personnel shall be proportional to the size of the ecosystem of the monitoring body (the number of code members, the size of code members, the nature and scope of the code members activities and the complexity and degree of risks of data processing made by code members).

1.5 An internal monitoring body is an internal department of the code owner. The internal monitoring body could not be setup within a code member.

An internal monitoring body shall provide information concerning its relationship to the code owner and shall evidence its impartiality. This must be demonstrated by evidence of an independent organization (the internal monitoring body shall be organized in a separate department of the code owner) with information barriers, separate reporting, separate personnel and management, accountability and function from other areas of the organisation. A framework which guarantees the independence of management, personnel and separation of responsibilities shall exist

The internal monitoring body shall have a separated allocated budget that it is able to manage independently.

1.6 Where a monitoring body uses sub-contractors, it shall ensure that sufficient guarantees are in place in terms of the knowledge, reliability and resources of the sub-contractor and obligations applicable to the monitoring body are applicable in the same way to the sub-contractor. The use of

subcontractors shall not remove the responsibility of the monitoring body. This must be demonstrated with evidence that may include:

a. written contracts or agreements to outline for example responsibilities, confidentiality, what type of data will be held and a requirement that the data is kept secure;
b. a clear procedure for subcontracting shall also be documented and include the conditions under which this may take place, an approval process and the monitoring of subcontractors; and
c. the monitoring body shall ensure sufficient documented procedures to guarantee the independence, expertise and lack of conflicts of interests of the sub-contractors.

1.7 The monitoring body shall demonstrate that it has the financial stability and resources required to carry out its operations and to meet its liabilities. The monitoring body shall demonstrate that the rules on its financing prevent any risks of undermining its independence or the performance of its tasks by a third party, in particular a code member or the code owner.

The monitoring body must provide evidence of financial independence from any code member (e.g.: a code member should not be a shareholder of the monitoring body).

The financial resources of the monitoring body shall be sufficient and proportional to the size of the ecosystem of the monitoring body (the number of code members, the size of code members, the nature and scope of the code members activities and the complexity and degree of risks of data processing made by code members).

1.8 The monitoring body shall provide evidence to demonstrate that it is accountable for its decisions and actions, for example, by setting out a framework for its roles and reporting procedures and its decision-making process to ensure independence. Such evidence must include but is not limited to job descriptions, management reports and policies to increase awareness among the personnel about the governance structures and the procedures in place (e.g. training).

1.9 Any decisions made by the monitoring body related to its functions shall not be subject to approval by any other organisation, including the code owner.

2. Conflicts of interest

Explanatory note: The requirements below aim to ensure that the monitoring body can deliver its monitoring activities in an impartial manner, identifying situations that are likely to create a conflict of interest and taking steps to avoid them. It will be for the monitoring body to explain the approach to safeguard impartiality and to evidence the mechanisms to remove or mitigate these risks as appropriate. Examples of sources of risks to impartiality of the monitoring body could be based on ownership, governance, management, personnel, shared resources, finances, contracts, outsourcing, training, marketing and payment of sales commission.

2.1 The monitoring body shall conduct its activities free of external influence, whether direct or indirect. It shall not seek or take instructions from any person, organization or association.

2.2 The monitoring body shall implement organizational and technical measures to identify, analyse, evaluate, treat, monitor and document on an ongoing basis any risks to impartiality of its personnel, organization, procedures, sub-contractors, etc. susceptible to create a conflict of interest.

2.3 The monitoring body shall have its own personnel chosen, directed and managed by itself or an independent provider not involved in the code (e.g. not the code owner or a code member, etc.). This

could be demonstrated by providing evidence, which includes job descriptions, personnel records, recruitment personnel resource allocations and line management arrangements.

2.4 The monitoring body, especially the internal monitoring body, shall be protected from sanctions or interference by the code owner, other relevant bodies or members of the code.

2.5 The monitoring body shall refrain from any action that is incompatible with its tasks and duties and must put in place safeguards to insure that it will not engage with an incompatible occupation.

3. Expertise

Explanatory note: The requirements below aim to ensure that the monitoring body possesses adequate competencies to undertake effective monitoring of a code. More detailed expertise requirements needs to be defined in the relevant code itself. Code specific requirements will be dependent upon such factors as: the size of the sector concerned, the different interests involved and the risks of the processing activities. These code specific requirements will be considered as part of the accreditation. In order for a monitoring body to meet the expertise requirements, it will need to demonstrate that its personnel have the required knowledge and experience in relation to the sector, processing activity, data protection legislation and auditing, in order to carry out compliance monitoring in an effective manner. This could be demonstrated to the CNPD with evidence that includes personnel job descriptions, specification requirements, qualifications, required or relevant experience, published reports etc.

3.1 The monitoring body shall demonstrate that personnel conducting its monitoring functions or making decisions on behalf of the monitoring body have appropriate sectoral and data protection expertise and operational experience, training and qualifications such as previous experience in auditing, monitoring or quality assurance.

3.2 The monitoring body shall demonstrate that it has an in-depth understanding, knowledge and experience with regard to the specific data processing activities in relation to the Code (sectoral and data protection expertise).

3.3 In addition to the above, the monitoring body shall demonstrate that it meets the relevant expertise requirements as defined in the code of conduct.

3.4 The monitoring body shall have a clear hiring framework in place to carefully assess a candidate's knowledge and experience according to the expectations set out in these accreditation requirements as well as those defined by the code itself (e.g. knowledge tests to be performed during the interview(s), check of diplomas / certificates, etc.).

3.5 In addition, the monitoring body shall demonstrate that the competencies, knowledge and experience of the personnel of the monitoring body to conduct its missions include at least the following:

a. For personnel with auditing expertise:
    - At least two years of audit experience (e.g. internal / external audit, accreditation audit, other regulatory audits, quality assurance, etc.).
b. For personnel with IT technical expertise:
    - a bachelor diploma or equivalent in the field of informatics, information systems, cybersecurity or similar, and
    - at least 2 years of experience in the field of information systems security.
c. For personnel with legal expertise
    - a Masters 2 diploma in the field of law, and
    - at least 2 years of experience in the field of personal data protection.

The number and proportion of personnel with auditing expertise, with IT technical expertise and with legal expertise employed by the monitoring body shall be adapted to the needs of the monitoring body, to the number and size of code members as well as to the complexity or degree of risk of the relevant data processing(s) covered by the code. The personnel with IT technical expertise or with legal expertise shall depend on whether it is necessary for the code at stake.

3.6 The monitoring body shall establish and implement a training programme for its personnel to ensure continuous professional development, which shall include at least training on sector-specific knowledge, data processing knowledge, protection of personal data, audit methods (procedures and techniques, documentation, quality review, etc.) and information security (standards, methods, best practices, risk management, etc.). This training programme shall be tailored to the needs of the monitoring body as well as to the needs of its personnel.

4. Established procedures and structures

Explanatory note: The requirements below aim to ensure that the proposals for monitoring are operationally feasible, by specifically outlining the monitoring process and demonstrating how it will deliver the code's monitoring mechanism. The monitoring body will need to demonstrate to the CNPD established procedures, structures and resources to assess the eligibility of controllers / processors to apply the code, monitor compliance with the code and to carry out periodic reviews of the code's operation. Monitoring procedures must take into account the risk raised by the data processing, complaints received and the number of members of the code. These procedures could lead to the publication of monitoring information including audit or summary reports or periodic outcomes reporting of findings. The monitoring body shall apply the corrective measures as defined in the code of conduct.

4.1 The monitoring body shall ensure that all processing activities that it carries out as part of its missions comply with the GDPR.

4.2 The monitoring body shall demonstrate that it has defined and implemented a procedure to check eligibility of members to comply with the code, for example, their processing of personal data falls within the scope of the relevant code of conduct.

4.3 The monitoring body shall have a defined and implemented procedure regarding ethics, deontology and independence rules applied by the monitoring body and its personnel.

4.4 The Monitoring body shall have a defined and implemented procedure regarding the hiring of personnel (including requirements on competencies, knowledge and experience) as well as the management of competencies in order to guarantee that personnel has the relevant diplomas and experiences/competencies required by the code and by these accreditation criteria.

4.5 The monitoring body shall demonstrate that it has defined and implemented a procedure to provide compliance monitoring to be carried out over a defined period taking into account such things as the complexity and risks involved, the expected number and size of code members, the geographical scope and complaints received.

4.6 The monitoring body shall demonstrate that their monitoring or review procedures define:

a. the criteria to be assessed (the eligibility of data controllers and data processors to adhere to the code, etc.);
b. the type of assessment to be used;
c. a procedure to document the findings and the audit report;
d. a procedure defining how findings generate actions concerning the (candidate) code member (e.g. non-admittance, suspension, exclusion) or recommendations to the (candidate) code member;
e. a procedure to monitor compliance with the Code after adherence.

Review procedures can include such things as audits, inspections, reporting and the use of self-monitoring reports or questionnaires.

4.7 The monitoring body shall demonstrate that it has defined and implemented a procedure for the investigation, identification and management of code member infringements to the code and additional controls to ensure appropriate action is taken to remedy such infringements as set out in the relevant code of conduct.

4.8 The monitoring body shall demonstrate that the monitoring procedure guarantees integrity and traceability of evidence when collecting the necessary information.

4.9 The monitoring body shall be responsible for the management of all information / documentation obtained or created during the monitoring process.

4.10 The monitoring body shall ensure that personnel will keep all information / documentation obtained or created during the performance of their tasks confidential, unless they are required to disclose or are exempt by law.

4.11 The monitoring body shall demonstrate that the audit results and conclusions issued are explained to the code member within a reasonable timeframe. An audit report shall be issued within a reasonable timeframe after the monitoring activity (audit) and shall be archived during the adherence period or more in case of litigations.

5. Transparent complaints handling

Explanatory note: Transparent and publicly available procedures and structures to handle complaints in relation to both code members and the monitoring body from different sources are an essential element for code monitoring. This process will be sufficiently resourced and managed, and personnel will demonstrate sufficient knowledge and impartiality. In order to meet these requirements, the monitoring body will need to provide evidence of a documented, independent, and transparent complaints handling process to receive, evaluate, track, record and resolve complaints within a reasonable time frame.

5.1 The monitoring body shall provide evidence of a clear framework for a publicly available, accessible and easily understood complaints handling, appeals and decision-making process. This shall be documented in a clear procedure indicating how to receive, manage / solve and respond to complaints about code members or about the monitoring body itself in a transparent and impartial way. This procedure shall be accessible to the public, including data subjects and code members.

5.2 The monitoring body shall acknowledge receipt of the complaint or appeal and provide the complainant with a progress report or the final decision of the investigation within a reasonable timeframe, such as three months from receipt of the complaint. This delay may be extended if the complaint is complex and more time is needed for the analysis; in this case, the monitoring body shall inform the complainant in detail about the reasons of the additional delay.

5.3 The monitoring body shall provide evidence of suitable and if necessary, immediate corrective measures, as defined in the code of conduct, in cases of infringement with the code to stop the infringement and avoid future re-occurrence. Such sanctions could also include, training, issuing a warning, report to the board of the member, formal notice requiring action, suspension or exclusion from the code.

5.4 The handling process for appeals shall include at least the following:

a. a description of the process for receiving, validating, investigating the appeal and deciding what actions are to be taken in response to it;
b. tracking and recording appeals, including actions undertaken to resolve them; and
c. ensuring that any appropriate action is taken in a timely manner.

5.5 The monitoring body shall keep detailed records of all received complaints (reception, handling, conclusion/decision, etc.) and makes these records accessible to the CNPD, which may access it at any time.

5.6 The monitoring body shall make all decisions and related reports publicly available in line with its complaints handling procedure (number and type of complains, corrective measures taken, type of sanctions as suspension or exclusion of a code member, etc.).

5.7 The monitoring body must inform the code member, the code owner and the CNPD about the measures taken and their justification without undue delay.

6. Communication with the CNPD

Explanatory note: The requirements below set out the information the monitoring body will provide to the CNPD. This includes information concerning any suspension or exclusion of code members and any substantial changes to its own status. It is envisaged that suspension or exclusion of code members will only apply in serious circumstances and code members would first have the opportunity to take suitable corrective measures as appropriate and agreed with the monitoring body. The monitoring body is accredited on the basis of fulfilling all requirements at the time of accreditation, and continuing to fulfil those requirements in order to effectively perform its function. Any subsequent substantial changes relating to the monitoring body's ability to function independently and effectively, its expertise and any conflict of interests would result in a review of its accreditation.

6.1 The monitoring body must keep records of all actions taken in one document always available and accessible to the CNPD.

6.2 The monitoring body shall communicate to the CNPD substantial changes to the basis of the accreditation that would impact the monitoring body's compliance to the accreditation requirements such as impartiality / independence, expertise or create conflicts of interests. Those changes may include but are not limited to:

a. its legal, commercial, ownership or organisational status and key personnel;
b. resources and location(s); and
c. any changes to the basis of accreditation.

6.3 The monitoring body shall report any substantial changes to the CNPD immediately, in writing and without undue delay.

6.4 Substantial changes must result in a review of the accreditation.

6.5 The monitoring body shall have a framework and a documented procedure for any corrective measures taken against a code member and for lifting the suspension or exclusion of a code member.

6.6 The Monitoring body must notify that code member and the CNPD of the outcome of the review or investigation immediately without undue delay and in writing. This outcome should contain at least:

a. the code member suspended or excluded and the reason of suspension or exclusion;
b. information outlining details of the infringement and actions taken; and

c. evidence that they have taken action in line with their suspension or exclusion process.

7. Code review mechanisms

Explanatory note: The requirements below aim to ensure that the monitoring body continuously reviews the code in accordance with the review mechanisms outlined in the code to ensure that the code remains relevant and continues to contribute to the proper application of the GDPR.

It is the role of the code owner to ensure the continued relevance and compliance of the code of conduct with applicable legislation. The monitoring body is not responsible for carrying out that task, but it shall contribute to any review of the code. As a result of a code review, amendments of or extensions to the code may be made by the code owner.

7.1 The monitoring body shall contribute to reviews of the code as required by the code owner.

7.2 The monitoring body shall have a framework including procedures for the assessment of the amendments of the code decided by the code owner to ensure that the code remains relevant to the members and continues to reflect GDPR principles application. Changes in the application and interpretation of the law and new technological developments shall be taken into consideration. The monitoring body shall apply and implement updates, amendments, and/or extensions to the Code, as decided by the code owner.

7.3 The monitoring body shall provide the code owner, the CNPD and any other establishment or institution referred to in the code of conduct with an annual report on the operation of the code. This report shall include:

a. information concerning new members to the code;
b. details of any suspensions and exclusions of code members;
c. confirmation that a review of the code has taken place and that following review no amendments to the code are required;
d. that there are no substantial changes to the monitoring body; and
e. Information concerning data breaches by code members, complaints managed and the type and outcome of monitoring functions that have taken place.

8. Legal Status

Explanatory note: The monitoring body can be set up or established in a number of different ways, however, the overarching principle is that whatever form the monitoring body takes, it must demonstrate sufficient financial and other resources to deliver its specific duties and responsibilities

The monitoring body will therefore have to provide evidence to the CNPD of its legal status including, where practical, the names of owners or named responsible officers and, if different, the names of the persons who control it. Fines could be administered for a monitoring body failing to deliver its monitoring functions and failing to take appropriate action when code requirements are infringed. A monitoring body will therefore demonstrate that it has the appropriate standing to carry out its role under Article 41(4).

8.1 The monitoring body shall be established in the European Economic Area.

8.2 The monitoring body shall be a legal entity, or a defined part of a legal entity such that it is legally responsible for its monitoring activities. The monitoring body shall agree to be responsible for its monitoring role to the supervisory authority for all its actions and decisions related to its activities.

8.3 The monitoring body must have sufficient financial, human and material resources and the procedures to ensure the continuity of its control activities for the duration of the accreditation and in accordance with the code.

9. Subcontracting

Explanatory note: The monitoring body can subcontract some of its activities to other parties, i.e. in relation to performing themonitoring activity. When using subcontractors, the obligations applicable to the monitoring body will be applicable in the same way to the subcontractor. The use of a subcontractor does not remove the responsibility of the monitoring body. The requirements below aim to ensure that the monitoring body's subcontracted activities are documented and have sufficient guarantees.

9.1 In case the monitoring body uses the services of a subcontractor, the regulatory body shall draw up, in writing, a contract or other legal act under the law of the European Economic Area, binding it to the subcontractor to ensure that all subcontracted missions are GDPR compliant. The use of subcontracting must not entail delegation of responsibility: the monitoring body shall in any case remain responsible for monitoring the code of conduct before the supervisory authority. The decision-making process cannot be subcontracted.

9.2 In case the monitoring body uses the services of a subcontractor, the regulatory body shall ensure that any subcontractor meets the requirements set out in these accreditation requirements, in particular with regard to independence, absence of conflict of interest and expertise.

9.3 In case the monitoring body uses the services of a subcontractor, the monitoring body must provide for the insertion of a special clause in the contract / legal act established with the subcontractor(s) in order to guarantee the confidentiality of any personal data, which could, if necessary, be brought to the attention of the subcontractor in the context of control activities.

9.4 In case the monitoring body uses the services of a subcontractor, the monitoring body shall ensure effective monitoring of the services provided by the contracting entities.

9.5 In case of termination of the contract, the monitoring body shall ensure that the subcontractors fulfill their data protection obligations.