Autorité de protection des données
Gegevensbeschermingsautoriteit

**Decision of the Secretary General nr. 01/2020 of the 24th of September 2020**

**Concerning** : **Accreditation requirements for code of conduct monitoring bodies (DOS-2019-06518)**

The Secretary General of the Belgian Data Protection Authority (hereafter: "Secretary General");

Considering the law of 3 December 2017 *on the creation of the Data Protection Authority*, and in particular article 20, §1, 6° (hereafter: "LCD");

Considering Regulation (EU) 2016/679 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 (General Data Protection Regulation, hereafter: "GDPR"), and in particular articles 41.3, 57.1.(p), and 64.1(c) GDPR;

Considering the law of 30 July 2018 *on the protection of natural persons in relation to the processing of personal data*, and in particular article 187 (hereafter: "LPP");

Considering the internal rules of procedure of the Belgian Data Protection Authority (hereafter: "Authority"), and in particular article 15 (hereafter: "ROP");

Considering the Guidelines 01/2019 on codes of conduct and monitoring bodies (hereafter "guidelines 01/2019") as adopted by the European Data Protection Board (hereafter: "EDPB") on the 4th of June 2019;

Considering the Opinion 2/2020 on the Belgium data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR adopted on 28 January 2020 by the EDPB;

Adopts on the 24th of September 2020 the following decision on the accreditation requirements for code of conduct monitoring bodies:

## I. Introduction

1. In accordance with article 41.1 GDPR and with the Guidelines 01/2019 adopted by the EDPB, national and transnational codes of conduct have to be monitored by a monitoring body that is accredited by the competent supervisory authority. The only exception to this rule lies in article 41.6 GDPR which stipulates that an accredited monitoring body is not necessary for processing carried out by public authorities or bodies.

2. In accordance with the Guidelines 01/2019, §64 and §65, the monitoring body can be either external or internal to the code owner[1]. Examples of internal monitoring bodies could include an ad hoc internal committee or a separate independent department within the code owner.

3. To be accredited by the Authority, a monitoring body has to fulfil all of the accreditation requirements set out in this decision based on the requirements of article 41.2 GDPR and section 12 of the Guidelines 01/2019. The monitoring body will retain its accreditation status unless the outcome of a review conducted by the Authority concludes that the requirements for accreditation are no longer met.

4. The Authority emphasises that pursuant to article 41.1 GDPR and the Guidelines 01/2019, accreditation as a monitoring body is only possible in relation to the subject matter of one or more specific codes of conduct.

5. By the present decision the Authority encourages the development of codes of conduct for micro, small and medium companies to foster a consistent implementation of the GDPR, to increase legal certainty for controllers and processors and to strengthen the trust of data subjects. The requirement for codes of conduct to be monitored by an accredited monitoring body should not be an obstacle to the development of codes of conduct. Therefore, the application of the accreditation requirements for monitoring bodies should take into account the specificities of each sectors' processing and should be as flexible as possible while abiding by the legal framework imposed by the GDPR, the Guidelines 01/2019 and the relevant Opinions of the EDPB.

[1] Code owner refers to the associations or other bodies who draw up and submit their code.

## II. Accreditation criteria

### 1. Independence and impartiality

The monitoring body shall demonstrate its independence and impartiality. The monitoring body shall demonstrate how its structure and its formal rules of appointment guarantee that it is able to act freely from instructions and that it shall be protected from any sort of interference or sanctions from the code members or the code owner as a consequence of the fulfillment of its tasks.This needs to be demonstrated within four main areas: legal and decision-making procedures, financial, organizational and accountability.

**Requirement 1.1**

Legal and decision-making procedures

- The legal structure of the monitoring body, including its ownership, must shield the monitoring body from external influence. This might be demonstrated for example by submitting the following documents, the articles of incorporation of the monitoring body and the articles of incorporation of the code owner.
- The monitoring body's decision-making procedures must ensure that the decision process from the conception of a decision to its implementation must shield the monitoring body from undue influence. The independence and impartiality of the decision-making procedure might be demonstrated for example by submitting the organigram of the monitoring body and the code owner; a description of the decision-making process that also points out to the roles and prerogatives of all parties involved in the decision-making process associated to a decision making procedure.

**Requirement 1.2**

Financial

The monitoring body shall demonstrate that the rules pertaining to its funding shall prevent the risk that a code member stops its financial contributions in order to avoid a corrective measure imposed by the monitoring body. This requirement can be fulfilled by providing for example explanations on the financial arrangements between the monitoring body and the members of the Code, including how the amount of contribution is calculated, the frequency at which the contribution is paid and the financial arrangement in case of withdrawal of a code member.

**Requirement 1.3**

Organisational

The monitoring body shall demonstrate that it is able to freely choose, direct and manage its staff in order to fulfill its tasks. Whether the choice of staff is made by the monitoring body itself or through an external provider, the hiring process, the management and dismissal of the personnel shall not be influenced by the code owner nor any code member. To fulfill this requirement, the monitoring body might for example provide evidence which includes job descriptions, personnel records, recruitment personnel resource allocations and line management arrangements .

An internal monitoring body shall provide additional information concerning its relationship to its code owner to evidence its independence and impartiality. This shall be demonstrated with evidence that may include :

- information barriers;
- separate reporting obligations;
- separate operational staff;
- separate management functions.

**Requirement 1.4**

Accountability

The monitoring body shall submit a document that explains its independence and impartiality in respect to:

- the code members;
- the association or other body referred to by Recital 98 of the GDPR and article 40.2 GDPR, which has submitted a code of conduct for approval

Accountability can be demonstrated by providing evidence that the monitoring body set out a framework for its roles and reporting procedures and its decision-making process to ensure independence. Such evidence could 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).

The monitoring body shall keep documents and proof of the respect of all the accreditation requirements and make them available to the Authority on request.

The monitoring body shall keep a register of the actions taken in the framework of its tasks including where appropriate, date, duration, types of action taken, code members concerned, reaction of the code member and outcome of the action.

This register shall be made available to the Authority on request.

## 2. Absence of conflicts of interest

**Requirement 2.1**

The monitoring body shall demonstrate the absence of any conflict of interest related to the personnel of the monitoring body and related to the monitoring body itself.

Conflicts of interest related to the personnel

To this end the monitoring body shall have in place a documented procedure to prevent, detect and eliminate potential conflicts of interest that its employees and management staff may have.

This procedure shall ensure that the previous and current functions of its employees and management staff do not prejudice their independence in the exercise of their tasks.

The absence of a conflict of interest of employees and management staff may be demonstrated for example through the procedures for recruitment, their remuneration, disciplinary sanctions, the length of their employment contract, their other professional occupations, internal staff rules and the provisions of their employment contract.

Conflicts of interest related to the monitoring body itself

The monitoring body shall refrain from any action that is incompatible with its tasks and duties and shall not take instructions from any person, organisation or association.

The Monitoring body shall identify situations that are likely to create a conflict of interest and set up internal rules in order to avoid conflicts of interest triggered by its activities, relationships, organisation or procedures. This requirement can be fulfilled by providing for example evidences such as the monitoring body's risk management strategy.

## 3. Expertise

**Requirement 3.1**

The monitoring body shall demonstrate the expertise to deliver the code of conduct's monitoring activities for the specific code that it will monitor.

The monitoring body shall provide evidence of adequate expertise in the following domains:

- in-depth understanding of data protection legislation and experience in its implementation ;
- knowledge and experience in the sector or processing activity for which it will act as a monitoring body;
- knowledge and experience in auditing to establish its capacity to monitor compliance of the code members with the code of conduct.

Additional expertise requirement can be defined by a code of conduct. The expertise of each monitoring body will be assessed in line with the expertise required by the particular code of conduct it monitors.

Expertise may be demonstrated for example by submitting evidence of adequately trained, educated and experienced staff in these domains. For example through the means of a diploma, certification and a proof of experience.

**Requirement 3.2**

The monitoring body shall demonstrate that its level of expertise is commensurate with the risks for data subjects, the sensitivity and complexity of the processing that takes places within the context of the code of conduct, the expected size of the sector concerned, and the expected number of code members.

**Requirement 3.3**

The monitoring body shall guarantee to maintain an appropriate legal, technical, and auditing expertise through continuous professional development and training of its staff.

## 4. Established procedures and structures

**Requirement 4.1**

The monitoring body shall demonstrate that it has an appropriate governance framework in place to assess the eligibility of controllers and/or processors that wish to join the code of conduct as a code member.

**Requirement 4.2**

The monitoring body shall demonstrate that it has an appropriate governance framework in place to continuously monitor compliance with the provisions of the code of conduct.

This governance framework provides at least for:

- a procedure that provides for plans for audits to be carried out over a defined period of time (recurring and *ad hoc*) based on criteria such as the risks for data subjects, the sensitivity and complexity of the processing that takes places within the context of the code of conduct, the expected number of code members and size of the sector concerned, the geographical scope and the received complaints;
- an audit methodology, which specifies the set of criteria to be assessed, the type of audits and the documentation of these findings;
- a procedure to identify, investigate and remedy infringements to the code of conduct;
- regular reporting obligations for the code members.

**Requirement 4.3**

The monitoring body shall demonstrate that it is composed of an adequate number of staff so that it is able to carry out its monitoring functions appropriately.

The amount and type of human resources required depend on the risks for data subjects, the sensitivity and complexity of the processing that takes places within the context of the code of conduct, the expected size of the sector concerned, and the expected number of code members. This requirement might be fulfilled by providing for example an organigram of the monitoring body describing the roles and number of staff assigned to each task.

**Requirement 4.4**

The monitoring body shall demonstrate that its employees are bound by a confidentiality duty in the course of their tasks.

**Requirement 4.5**

The monitoring body shall demonstrate that it has sufficient funding and financial sustainability to fulfill its tasks (as per requirement 8.4)

## 5. Complaints and Sanctions

**Requirement 5.1**

The monitoring body shall establish a procedure to handle complaints. This procedure should also be detailed in the monitored code of conduct.

This procedure shall deal with complaints introduced by data subjects, and body, organisation or association referred to in article 80 of the GDPR against the code members.

This procedure shall stipulate the form of the complaint (in writing or electronically), a point of contact in charge of handling the complaint, the process of handling the complaint, and the different outcomes of resolution as determined in the monitored code of conduct.

This procedure shall be made publicly available and transparent.

**Requirement 5.2**

The monitoring body shall acknowledge receipt of the complaint.

The complainant shall be notified on the progress or outcome of the complaint at the latest within three months from the receipt of its complaint.

The period to resolve the complaint may be extended by a reasonable period where necessary, taking into account the complexity of the complaint. The monitoring body shall inform the complainant of any such extension within three months of receipt of the complaint, together with the reasons for the delay.

**Requirement 5.3**

The monitoring body shall establish a register of all complaints received and ensure that decisions of the body are made publicly available. Furthermore, the monitoring body shall publish, on a regular basis, statistical data with the result of the monitoring activities, such as the number of complaints received, the type of infringements and the corrective measures issued.

**Requirement 5.4**

The monitoring body shall provide evidence of suitable corrective measures, as defined in the code of conduct, in cases of infringement to 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.

## 6. Communication

**Requirement 6.1**

The monitoring body shall annually communicate to the Authority a report with an overview its activities and decisions.

The monitoring body shall also communicate to the Authority any action taken in case of infringement of the code of conduct and the reasons for this action. The frequency of this communication depends on the risks for data subjects, the sensitivity and complexity of data processing that takes places within the context of the code of conduct, the expected size of the sector concerned, the expected number of code members, the seriousness and frequency of infringements and the measures taken as set by the Code of Conduct itself.

**Requirement 6.2**

The monitoring body shall have a procedure in place to communicate to the Authority without delay:

- any substantial change to its organisation and/or structure which could affect its ability to perform its function impartially, independently and effectively. Such substantial changes may include:
    - a change in legal, commercial and organisational status;
    - a change in the organisation's senior management and key staff;
    - a change in the financial resources and location of the monitoring body;
    - Significant changes in the number of code members
- any suspension or exclusion of a code members;
- any substantial infringement to the code of conduct as well as information outlining details of the infringement and action taken.

**Requirement 6.3**

The monitoring body shall have a procedure in place to make publicly available the following information:

- a general description of the funding mechanisms of the monitoring body;
- information about the procedures for handling complaints;
- information about the monitored code of conduct and the monitoring mechanism (including the procedures mentioned in requirements 6.1, 6.2, 7.1 and 7.2, the rules and procedures for granting,

maintaining, suspending, excluding and withdrawing code membership) as set out in the rules and procedure of the code of conduct monitored;

- all corrective measures leading to exclusion from the code of conduct as set out in the rules and procedure of the code of conduct monitored.

## 7. Review Mechanisms

**Requirement 7.1**

The monitoring body shall set up procedures to take into account a modification of the legal framework impacting the substance of the provisions of the code of conduct.

**Requirement 7.2**

The monitoring body shall contribute appropriately to the review of the code of conduct's operation and set up mechanisms to enable feedback to the code owner and to any other entity referred to in the code of conduct. For example, set up an annual reporting obligation on the operation of the Code to the code owner and any other entity referred to in the Code of conduct

## 8. Legal status and organisational structure

**Requirement 8.1**

The monitoring body shall indicate whether it acts as an internal or external monitoring body in relation to the code owner.

**Requirement 8.2**

Regardless of its legal form, the monitoring body shall have appropriate legal standing to be held accountable, to carry out its role under article 41(4) GDPR and to be capable of being fined as par article 83.4.c) GDPR.

**Requirement 8.3**

The monitoring body shall be established within the European Economic Area ("EEA").

**Requirement 8.4**

The monitoring body shall demonstrate the sustainability and continuity of its monitoring activities over time and specifically in relation to the fact that it has set up procedures to ensure:

- sufficient financial resources (as per requirement 4.5);
- sufficient staff to fulfill its tasks (as per requirement 4.3);

**Requirement 8.5**

The monitoring body shall formally commit to comply with all relevant legislation and in particular the provisions of the GDPR.

**Requirement 8.6**

When marks, signs, or similar tools are used to warrant compliance with the code of conduct, the monitoring body shall initiate suitable action in case of any fraudulent use (E.g. incorrect references or misleading use) of such marks, signs, or similar tools.

## 9. Subcontractors

**Requirement 9.1**

When the monitoring body engages a subcontractor to fulfills some of its tasks, the monitoring body remains responsible for all activities sub-contracted.

**Requirement 9.2**

The monitoring body shall specify the tasks and roles that the subcontractors will carry out when it applies for accreditation.

**Requirement 9.3**

The monitoring body shall demonstrate that the subcontractor satisfies all relevant requirements set out in this decision and in particular requirements 1; 2; 3; 8.5.

The monitoring body shall demonstrate that the subcontractor is effectively bound by these requirements and can deliver compliance on them.

**Requirement 9.4**

Without prejudice to requirement 6.3, the monitoring body shall have a procedure in place to communicate to the Authority without delay all substantial changes relating to a subcontractor that have an impact on the organisation and/or structure of the monitoring body which could affect its ability to perform its function effectively. Such substantial changes may include:

- the termination of the agreement with the subcontractor;
- the replacement of the subcontractor by a new one.

## 10. Language

**Requirement 10.1**

All supporting documentation to demonstrate compliance with these requirements shall be submitted in Dutch, French or any different language at the discretion of the Authority.

(signed) David Stevens
Secretary General