Bld. Gen. Gheorghe Magheru Nr. 28-30, Sector 1, Cod poştal 010336, Bucureşti ; Tel. +40.31.805.9211; Fax:+40.31.805.9602 www.dataprotection.ro; e-mail: anspdcp@dataprotection.ro

DECISION no. 64 of 17th of May 2023

on the approval of the

Requirements for accreditation of the monitoring body of the codes of conduct

pursuant to Article 41 of Regulation (EU) 2016/679

Having regard that the provisions of Article 40 (4) of 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), hereinafter referred to as the General Data Protection Regulation, establish that a code of conduct includes mechanisms that allow the monitoring body to carry out the mandatory monitoring of compliance with its provisions by controllers or processors who undertakes to apply it, without prejudice to the tasks and powers of the supervisory authorities that are competent under Article 55 or 56 of the General Data Protection Regulation,

Since Article 41 (1) of the General Data Protection Regulation establishes that the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority,

Considering the provisions of Article 24 (3), Article 28 (5) and Article 32 (3) of the General Data Protection Regulation, according to which the adherence to an approved codes of conduct can be used as an element to demonstrate the compliance with the obligations by the controller and the processor, as well as the existence of sufficient safeguards for the implementation of adequate technical and organisational measures, so that the processing complies with the requirements set out in the same regulation and ensures the protection of the rights of the data subject,

Having regard to the provisions of Article 57 (1) letter p) and of Article 64 (1) letter c) of the General Data Protection Regulation according to which the supervisory authority drafts and publishes the requirements for accreditation of a body for monitoring codes of conduct pursuant to Article 41,

Taking into account the requirements provided by Article 41 (2) of the General Data Protection Regulation, which a body for monitoring the compliance with a code of conduct shall fulfill in order to be accredited,

Considering the provisions of Article 41 (4) of the General Data Protection Regulation according to which the monitoring body shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code and it shall inform the competent supervisory authority of such actions and the reasons for taking them,

Having regard to the provisions of Article 41 (5) of the General Data Protection Regulation according to which the competent supervisory authority shall revoke the accreditation of a body if the conditions for accreditation are not, or are no longer met or where actions taken by the body infringe the General Data Protection Regulation,

Taking into account the provisions of Article 41 (6) of the General Data Protection Regulation according to which Article 41 of this Regulation shall not apply to processing carried out by public authorities and bodies, as defined in Article 2 (1) letter a) of Law no. 190/2018 on implementing measures to 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), with subsequent amendments,

Having regard to the Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, hereinafter referred to as the Guidelines 1/2019, and to the Guidelines 04/2021 on Codes of Conduct as tools for transfers, issued by the European Data Protection Board, hereinafter referred to as the Board, which contain the main criteria for approving codes of conduct, including criteria regarding the existence of mechanisms that allow the monitoring body to carry out the mandatory monitoring of compliance with the provisions of the code by the controlleras or processors who undertake to apply it, without prejudice to the tasks and powers of the supervisory authorities that are competent under Article 55 or Article 56 of the General Data Protection Regulation,

Condering the provisions of Article 41 (3) of the General Data Protection Regulation according to which the competent supervisory authority shall submit the draft requirements for accreditation of a body to the Board pursuant to the consistency mechanism referred to in Article 63 of the Regulation,

In consideration of the Opinion no. 3 of 3rd of February 2023 of the Board on the draft Requirements for accreditation of a monitoring body of codes of conduct, issued under Article 41 of Regulation (EU) 2016/679, communicated to the National Supervisory Authority for Personal Data Processing on the 16th of February 2023,

Based on the Note of the Legal and Communication Department no. 136 of the 31st of August 2020 on the draft Decision on the approval of the Requirements for accreditation of a monitoring body of codes of conduct, pursuant to Article 41 of Regulation (EU) 2016/679,

Pursuant to the provisions of Article 3 (5) and (6), Article 10 letters a)-d), Articles 14-19 of Law no. 102/2005 on the set up, organisation and functioning of the National Supervisory Authority for

Personal Data Processing, republished, as well as the Regulation on the organisation and functioning of the National Supervisory Authority for Personal Data Processing, approved by Decision no. 16/2005 of Standing Bureau of the Senate, with further amendments and completions,

the president of the National Supervisory Authority for Personal Data Processing issues this decision.

Article 1

The Requirements for accreditation of a monitoring body of codes of conduct pursuant to Article 41 of Regulation (EU) 2016/679, provided in the annex which is an integral part of this decision, are approved.

Article 2

This decision enters into force on thedate of publication in the Official Journal of Romania, Part I.

President of the National Supervisory Authority for Personal Data Processing,

Ancuţa Gianina Opre

Annex

Requirements for accreditation of a monitoring body of codes of conduct pursuant to Article 41 of Regulation (EU) 2016/679

CHAPTER 1: GENERAL PROVISIONS

Section 1 – Definitions

1. *Code owner* – associations or other bodies who draw up and submit their code to the Competent Supervisory Authority for approval.
2. *Monitoring body* – a body/committee or a number of bodies/committees (internal or external to the code owners) who carry out a monitoring function to ascertain and assure that the code is complied with as per Article 41 of the General Data Protection Regulation.
3. *Accreditation* – ascertainment by decision of the president of the Competent Supervisory Authority that the proposed monitoring body meets the requirements set out in Article 41 of 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) to carry out the monitoring of compliance with a code of conduct. The accreditation of a monitoring body applies only for a specific code.
4. *National code* – code which covers processing activities contained in one Member State.
5. *Transnational code* – code which covers processing activities in more than one Member State.
6. „*Competent SA*" – supervisory authority which is competent as per Article 55 of the General Data Protection Regulation, namely the National Supervisory Authority for Personal Data Processing.
7. „*Concerned SA*" – supervisory authority provided in Article 4 point (22) of General Data Protection Regulation.

Section 2 – General consideration and legal grounds

1. Pursuant to Article 41 paragraph (1) of General Data Protection Regulation, the codes of conduct shall be monitored by a monitoring body which is part of the code of conduct and is accredited by the Competent Supervisory Authority.

2. According to Article 41 paragraph (6) of General Data Protection Regulation, the processing carried out by public authorities and bodies, as defined in Article 2 paragraph (1) of Law no. 190/2018 on implementing measures to 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), with subsequent amendments, are not subject to the obligation mentioned in paragraph (1). This exception does not affect the implementation of the effective mechanisms for monitoring the code, such as adapting the existing audit requirements in order to include the monitoring of the code.

3. In accordance with paragraphs 64 and 65 of the Guidelines 1/2019, the monitoring body can be external or internal, provided that, in both cases, the respective body fulfils these accreditation requirements. An internal monitoring body could include an internal ad hoc committee or a separate, independent department within the code owner. An internal monitoring body cannot be setup within a code member.

4. In order to be accredited, the monitoring body must meet these accreditation requirements, established in accordance with Article 41 paragraph (2) of the General Data Protection Regulation, section 12 of Guidelines 1/2019 and Guidelines 04/2021 and approved by the European Data Protection Board by Opinion no. 3/2023.

5. The monitoring body that has an adequate level of expertise in relation to the subject of the specific code of conduct that it monitors shall be accredited. The monitoring of another specific code of conduct requires a new accreditation of that body.

6. Where it is found that the accreditation requirements are no longer met or that the measures taken by the body in question infringes the General Data Protection Regulation, the Competent Supervisory Authority shall revoke the accreditation of the body referred to in paragraph (1), according to the procedure provided for in Chapter IV of these requirements.

7. The accreditation shall be renewed whenever there are changes that affect the ability to exercise the functions of independence and efficiency of the monitoring body or the modification of the extension of the code of conduct. In case of substantial changes to the monitoring body relating to the monitoring body’s ability to function independently and effectively, such a review will always be conducted.

8. The monitoring body shall submit to the Competent Supervisory Authority an application for the renewal of accreditation, accompanied by all the necessary documentation to demonstrate the fulfilment of the requiremetns and indicating, in particular, the updated information required.

9. The accreditation and accreditation renewal procedure is carried out in writing, and the entire related documentation shall be submitted to the Competent Supervisory Authority in Romanian.

10. The application for accreditation shall include the information necessary to identify and contact the monitoring body and their legal representatives, in accordance with legal status of the body.

CHAPTER II: ACCREDITATION REQUIREMENTS FOR MONITORING BODIES

Section 1. Independence

Subsection 1.1: Independence and impartiality

1. According to Article 41 paragraph (2) letter a) of the General Data Protection Regulation, the monitoring body shall demonstrate to the Competent Supervisory Authority that it is adequately independent from the members of the code and the profession, industry or sector to which the code applies.

2. The independence of the monitoring body may be demonstrated by 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 the monitoring of compliance with a code of conduct in complete autonomy, without being directly or indirectly influenced or subjected to any form of pressure that might affect its decisions. This means that the monitoring body should not be in a position to receive any instructions regarding the exercise of its task from code members, the profession, industry or sector to which the code applies or from the code owner itself.

3. The monitoring body must demonstrate impartiality and independence in relation to four main areas: legal and decision-making procedures, financial resources, organisational resources and structure and accountability.

Subsection 1.2: Organisational structure and functioning

1. Where an internal monitoring body is proposed, there should be separate staff and management, accountability and function from other areas of the organisation. This may be achieved in a number of ways, for example, the use of effective organisational and information barriers and separate reporting management structures for the association and monitoring body.

2. The monitoring body shall assume the responsibility for its activities, shall be able to act free from instructions and shall be protected, both from the code owner and from the code members, against any dismissal or sanction, whether direct or indirect, for the performance of its duties.

3. Independence could require that an external counsel or other party having participated in the drafting of the code of conduct, would need to demonstrate that there were appropriate safeguards in place to sufficiently mitigate a risk of independence or a conflict of interest. The monitoring body would need to provide evidence as to the appropriateness of the mechanisms which would satisfactorily identify and mitigate such risks.

4. A monitoring body will need to identify risks to its independence on an ongoing basis, such as its activities and the risks to its relationships.

5. If a risk to independence is identified, the monitoring body should demonstrate how it removes or minimises such risk and uses an appropriate mechanism for safeguarding the independence.

Subsection 1.3: Budget and resources

1. The monitoring body shall demonstrate the full autonomy for the management of the budget and other resources, in particular in cases where the monitoring body is internal. The method of obtaining the financial resources cannot affect the independence of the monitoring body.

2. The monitoring body shall act independently in its choice and application of sanctions against a controller or processor adhering to the code.

3. Whether the monitoring body is internal or external, the monitoring body shall have a specific separated budget and shall be able to manage its budget and resoursece independently from code owners and members within the scope of the code in performing its tasks and exercising its powers.

4. The resources of the monitoring body shall be proportionate to the number and size of code members, nature and purpose of the activity, as well as the complexity or degree of risk associated to the relevant data processing.

Subsection 1.4: Accountability

1. The monitoring body shall demonstrate that it is accountable for its decisions and actions in order to be considered independent.

2. The monitoring body shall demonstrate that its staff has the necessary knowledge and experience in the activities which are subject matter of the code, data protection legislation and conducting audits in order to meet the monitoring requirements in an effective manner.

3. Any decision taken by the monitoring body in relation to its functions cannot be subject to the approval of the code owner or any other entity.

4. The monitoring body shall provide evidence to the Compentent Supervisory Authority on its independence in relation to accountability. Such evidence can be demonstrated by working procedures, formal rules for appointment and tasks of the personnel, internal procedures (such as procedures for personnel training), allocation of appropriate roles and structures in the organisation, description of the decision-making process by the montoring body.

5. The monitoring body and its staff shall respect the confidentiality of the information and documents obtained or created in connection with the exercise of their tasks, except for the situations provided for by the law.

Section 2. Conflict of interest

1. According to Article 41 paragraph (2) letter d) of the General Data Protection Regulation, the monitoring body shall demonstrate to the Competent Supervisory Authority that its tasks and duties do not result in a conflict of interests. 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 has previously worked for the code owner or for any of the organisations adhering to the code.

2. The code owners shall demonstrate that the proposed monitoring body will refrain from any action that is incompatible with its tasks and duties and that safeguards are put in place to ensure that it will not engage with an incompatible occupation. Thus, the procedures and measures put in place to avoid the conflict of interest shall ensure that the monitoring body shall refrain from any action incompatible with its tasks and duties.

3. The monitoring body must remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from any person, organisation or association.

4. The monitoring body shall have its own staff which are chosen by them or some other independent body of the code and it shall be subject to the exclusive direction of those bodies only.

5. The staff of the monitoring body must report internally any situations that could present risks on affecting the independence or creating conflict of interest.

6. In the case of an internal monitoring body, it shall be protected from any sort of sanctions or direct or indirect interference by the code owner, other relevant bodies, or members of the code as a consequence of the fulfilment of its tasks.

Section 3: Expertise

1. According to Article 41 paragraph (1) of the General Data Protection Regulation, the monitoring of compliance with a code of conduct pursuant to Article 40 of the same regulation shall be carried out by a body which has an appropriate level of expertise necessary to perform its role effectively and that demonstrates this to the Competent Supervisory Authority. Therefore, this may be demonstrated by expertise, experience and knowledge in respect of data protection law, as well as of the particular sector or processing activity.

2. Evidence of the level of expertise should include details as to the knowledge and experience of the body in respect of data protection law, as well as of the particular sector or processing activity, such as:

- being able to point a previous experience of acting in a monitoring capacity for a particular sector;
- an in-depth understanding of data protection issues and expert knowledge of the specific processing activities which are the subject matter of the code.

3. Futhermore, other factors such as the size of the sector concerned, the different interests involved and the risks of the processing activities should be taken into account.

4. The staff of the proposed monitoring body shall also have appropriate operational experience and training for carrying out the monitoring of compliance such as in the field of auditing, monitoring, or quality assurance activities.

Section 4: Established procedures and structures

1. According to Article 41 paragraph (2) letter b) of the General Data Protection Regulation, the monitoring body shall have appropriate governance structures and procedures which allow it to adequately:

- assess for eligibility of controllers and processors to adere to and apply the code,
- to monitor compliance with its provisions by the controllers and processors, and
- to carry out reviews of the code's operation.

2. The procedures and structures to actively and effectively monitor compliance by members of the code can include random or unannounced audits, annual inspections, regular reporting and the use of questionnaires.

3. The monitoring procedures can be designed in different ways as long as they take into account factors such as the risks raised by the data processing in scope of the code, complaints received or specific incidents and the number of members of the code.

4. Consideration could be given to the publication of audit reports as well as to the findings of periodic reporting from controllers and processors within the scope of the code.

5. The code owners shall also need to demonstrate that the proposed monitoring body have adequate resources and staffing to carry out its tasks in an appropriate manner.

6. The resources shall fulfill also the conditions provided under Section 1.3 paragraph (4) of these requirements.

Section 5: Transparent complaints handling

1. According to Article 41 paragraph (2) letter c) of the General Data Protection Regulation, the monitoring body will need to establish effective procedures and structures which can deal with complaints handling in an impartial and transparent manner and within reasonable deadlines. Following the complaint received, the monitoring body shall inform the complainant on the progress or the outcome of the complaint within three months from the date of receiving the complaint.

2. The monitoring body shall have a publicly accessible complaints handling process, as well as sufficient resources to manage complaints and to ensure that decisions of the body are made publicly available. At the same time, the decisions of the monitoring body shall be publicly available according to complaints handling procedure. The monitoring body shall make available to the Competent Supervisory Authority or, as the case may be, to the concerned supervisory authorities, the internal records resulting from the handling of complaints, at their request.

3. The monitoring body shall have effective procedures to ensure compliance with the code by controllers or processors, such as the competence to impose immediate corrective measures in order to cease the infringement and to avoid future recurrence, such as:

- temporary suspension of the member from the code until remedial action is taken;

- definitive exclusion of a controller or processor from the code when it acts outside the terms of the code of conduct;

- issuing a warning;

- report to the European Data Protection Board of the concerned member in the case of transnational code monitoring and reporting to the Competent Supervisory Authority in case of national codes;

- issuing a formal notice requiring the implementation of specific actions within a specified deadline.

4. These measures can be publicised by the monitoring body, especially where there are serious infringements of the code.

5. Where required, the monitoring body shall inform the code member, the code owner, the Competent Supervisory Authority and all concerned supervisory authorities about the measures taken and its justification without undue delay.

6. In the case where a Lead Supervisory Authority for a transnational code member is identifiable, the monitoring body should also appropriately inform this supervisory authority as to its actions.

Section 6: Communication with the National Supervisory Authority for Personal Data Processing

1. The monitoring body needs to have a procedure regarding the effective communication of any actions carried out by a monitoring body, with reference to the code of conduct which it monitors, to the Competent Supervisory Authority and, as the case may be, to other supervisory authorities.

2. The communication with the Competent Supervisory Authority may include aspects such as the decisions concerning the actions taken in cases of infringement of the code by a code member, providing periodic reports on the code monitoring, or providing review or audit findings of the code.

3. The measures taken by the monitoring body do not affect the tasks and powers of the Competent Supervisory Authority and Chapter VIII of the General Data Protection Regulation.

Section 7: Review Mechanisms

1. The code of conduct shall set out appropriate review mechanisms to ensure that the code remains relevant and continues to contribute to the proper application of the General Data Protection Regulation.

2. The monitoring body shall have procedures by which review mechanisms shall be put in place in order to adapt to any changes in the application and interpretation of the law or where there are new technological developments which may have an impact upon the data processing carried out by its members or the provisions of the code.

3. The activity of updating the code of conduct falls under the responsibility of the code owner.

Section 8: Legal status of the monitoring body

1. The proposed monitoring body - internal or external - and related governance structures shall have an adequate legal status so that it can demonstrate that they have the adequate competences to carry out their role under Article 41 paragraph (4) of the General Data Protection Regulation.

2. The proposed monitoring body shall have an adequate legal status that can ensure that the measure of the fine provided by the provisions of Article 83 paragraph (4) letter c) of the General Data Protection Regulation can be applied and implemented.

3. The monitoring body shall demonstrate that it is able to deliver the code of conduct's monitoring mechanism over a suitable period of time. In order to demonstrate the continuity of the monitoring function, the monitoring body shall demonstrate that it has sufficient financial and other resources and the necessary procedures.

4. The monitoring body shall not be allowed to recourse to subcontractors.

5. The legal status is demonstrated with documents appropriate to the structure of the monitoring body according to the applicable legislation.

6. The proposed monitoring body shall have the premises established in the European Economic Area.

CHAPTER III: APPROVED CODES

1. Following the approval of the code of conduct, the monitoring body shall work closely with the Competent Supervisory Authority in terms of the reporting requirements arising from the code.

2. The monitoring body shall act as the lead contact and coordinator in terms of any issues which may arise in relation to the code.

3. The nature and content of the code shall determine the roles of the relevant stakeholders in terms of ensuring compliance with the code and the General Data Protection Regulation, without prejudice to the tasks and competences of the Competent Supervisory Authority in this respect.

4. Any subsequent amendments or extensions to the code of conduct shall be subject to the approval of the Competent Supervisory Authority or other supervisory authority, as appropriate. Changes that affect the application of the code and that require approval could include, for example, adding a new code rule, but not updating a reference to the name of an organisation, or other minor changes that do not impact on the operation of the code. Changes that do not affect the application of the code shall be brought to the attention of the Competent Supervisory Authority.

5. Any new monitoring bodies of the code shall be subject to the accreditation by the Competent Supervisory Authority.

Chapter IV: REVOCATION OF A MONITORING BODY

1. When a monitoring body does not comply with these requirements for accreditation or the measures taken by the body infringes the provisions of the General Data Protection Regulation, the Competent Supervisory Authority shall revoke the accreditation of the monitoring body under Article 41 paragraph (5) of the General Data Protection Regulation.

2. Prior to taking the revocation measure, the Competent Supervisory Authority shall give the monitoring body the opportunity to urgently address the issues or to make improvements as appropriate within an agreed timescale.

3. In the case of a sole monitoring body for a code, the consequences of revoking the accreditation may include the suspension or permanent withdrawal of that code due to the loss of the required compliance monitoring.

4. In the case of transnational codes, the Competent Supervisory Authority informs all the concerned supervisory authorities about the adoption of the measure of revoking the accreditation of the monitoring body. Similarly, for such codes, taking into account the importance of the effectiveness of the monitoring body and of that code, the concerned supervisory authority shall inform the Competent Supervisory Authority in cases where a controller is found to be non-compliant with the code.

5. In cases which involve transnational codes, the Competent Supervisory Authority shall, before agreeing to setting parameters with the monitoring body to address the issues raised, liaise with concerned supervisory authorities on the matter.

6. The decision to revoke a monitoring body in the case provided in paragraph (5) shall be communicated to all concerned supervisory authorities and the European Data Protection Board.

7. The code owner must include appropriate provisions in the code to provide for the applicable procedure in the event of revoking a monitoring body.

Chapter V: PUBLIC SECTOR CODES

1. According to Article 41 paragraph (6) of the General Data Protection Regulation, the monitoring of approved codes of conduct will not apply to processing carried out by public authorities or bodies.

2. The exemption provided in paragraph (1) does not in any way dilute the requirement for the implementation of effective mechanisms to monitor a code, which could be achieved by adapting the existing audit requirements to include monitoring of the code.

Published within the Official Gazette no. 527 as of 14th of June 2023