STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 11665
10 maart
2021

NL accreditation requirements for GDPR code of conduct monitoring bodies, Autoriteit Persoonsgegevens

The Dutch Data Protection Authority (in Dutch: de Autoriteit Persoonsgegevens, hereinafter: AP),

Whereas Article 41(1)of the General data Protection Regulation (GDPR) 2016/679 of 26 April 2016 states that compliance monitoring of approved codes of conduct may be carried out by an impartial monitoring 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;

Whereas Article 41 (3) GDPR provides that the competent supervisory authority submits the draft requirements for accreditation of a body referred to in paragraph 1 of this Article to the Board pursuant to the consistency mechanism referred to in Article 63 and Article 64 (1) (c);

Whereas Article 57, opening lines and under p, GDPR, stipulates that each supervisory authority is responsible for drawing up and publishing the requirements for the accreditation of a body for the supervision of codes of conduct on the basis of Article 41 of the GDPR;

Whereas Article 6 (2) of the Dutch General Data Protection Regulation Implementation Act (in Dutch: Uitvoeringswet Algemene verordening gegevensbescherming, hereinafter: UAVG) stipulates that the AP is the supervisory authority referred to in Article 51 (1) of the GDPR;

Whereas the European Data Protection Board (EDPB) has adopted: Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, in particular para 60;

Whereas the Guidelines 1/2019 set out a number of requirements which the proposed monitoring body needs to meet in order to gain accreditation. In particular the following requirements should be met:
- Demonstrate independence and expertise in relation to the subject matter of the code as per *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).*
- Demonstrate to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interest as per *Article 41(2)(d).*

Whereas the EDPB has adopted: 'Opinion 07/2020 on the draft decision of the competent supervisory authority of Netherlands regarding the approval of the requirement for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR', adopted on 23 July 2020.

Has on 23 February 2021 adopted the following decision on the accreditation requirements for code of conduct monitoring bodies:

Accreditation requirements

By the present decision the AP 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.

The AP reserves the right to conduct a risk-based review of the monitoring body to ensure that the body still meets the requirements for accreditation. Such a review could be initiated by (but is not limited to): amendments to the code of conduct, substantial changes to the monitoring body or the

monitoring body failing to deliver its monitoring functions. 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.

The monitoring body will retain its accreditation status unless the outcome of this review concludes that the requirements for accreditation are no longer met.

The introduction of a new or additional monitoring body for a code of conduct will require the new body to be assessed in line with the accreditation criteria.

The requirements listed in this document shall apply to a monitoring body regardless of whether it is an internal or external body, unless the requirement states otherwise.

1 Independence

Explanatory note:
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 fulfilment of its tasks.

The requirements below set out what constitutes independence. This needs to be demonstrated within four main areas: legal and decision making procedures, financial, organisational and accountability. 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 members of the code or its code owner.

Monitoring bodies wills be structured and managed to safeguard their independence and impartiality and will be required to demonstrate this to the AP in their submission.

Internal bodies shall be required to provide evidence to ensure that the independence of their monitoring activities are not compromised.

Requirements:

1.1 Legal and decision-making procedures

1.1.1 Legal and decision-making procedures
- The legal structure of the monitoring body, including its ownership, must shield the monitoring body from external influence with respect to the code owners and the code members. This might be demonstrated for example by submitting the following documents, the articles of incorporation (the set of formal documents filed with a government body to legally document the creation of a corporation) of the monitoring body and the articles of incorporation of the code owner and by demonstrating that the duration, or expiration of the mandate of the monitoring body is fixed in such a way as to prevent overdependence on a renewal or fear of losing the appointment, to an extent that adversely affects the independence in carrying out the monitoring activities by the monitoring body.
- The monitoring body shall demonstrate any legal and economic links that may exist between the monitoring body and the code owner or code members, as well as with regard to the profession, industry or sector to which the code applies.
- 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.
- The monitoring body could be an internal or external body as long as evidence can be provided of adequate procedures and rules that allow monitoring of compliance with a code independently and without undue pressure or influence from the code owner or the code members.

1.1.2. The monitoring body shall demonstrate that it will act independently in its choice and application of its actions and sanctions. 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).

1.1.3. An internal monitoring body shall provide information concerning its relationship to its larger entity (in particular the code owner) and shall evidence its impartiality. This could be demonstrated with evidence that may include information barriers, separate reporting and separate operational and management functions.

1.1.4. The monitoring body shall demonstrate organisational independence, for example, an internal monitoring body may use different logos or names where appropriate, information barriers and separate reporting structures.

1.1.5. The monitoring body shall not provide any services to code members that would adversely affect its independence.

1.1.6. 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.

1.2 Financial

1.2.1. The monitoring body shall demonstrate that it has the financial stability and resources, for the operation of its activities and to meet its liabilities. The resources should be proportionate to the expected number, size and complexity of code members (as monitored entities), the nature and scope of their activities (which are the subject of the code) and the risk(s) associated with the processing operation(s).

1.2.2. The monitoring body shall be able to manage their budget and resources independently and effectively monitor compliance without any form of influence from the code owner or code members.
This could be demonstrated with evidence showing that the means by which it obtains financial support should not adversely affect its independence. The monitoring body would, for instance, 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 contribution to it, in order to avoid a potential sanction from the monitoring body.

1.2.3. The monitoring body shall demonstrate to the AP the means by which it obtains financial support for its monitoring role and explain how this does not compromise its independence. This could be evidenced by delivering contractual clauses or other documentation that demonstrates how the monitoring body obtains financial support for its monitoring role.

1.3 Organisational

1.3.1. The monitoring body shall demonstrate that it has adequate resources (including technical resources)and personnel to effectively perform its tasks, the resources should be proportionate to the expected number and size of code members, as well as the complexity or degree of risk of the relevant data processing, 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.

1.3.2. The monitoring body shall provide evidence during the application process that their personnel can act independently and without undue pressure or influence in relation to:
a. supervision of resources and finances of the monitoring body;
b. decisions on and performance of compliance monitoring; and
c. safeguarding of impartiality.
Such evidence can include but is not limited to documented recruitment/appointment processes, job descriptions, risk registers, risk treatments, meeting minutes and other documented processes as appropriate.

1.3.3. 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. Even when subcontractors are used, the monitoring body shall ensure effective monitoring of the services provided by the contracting entity. The use of subcontractors does not remove or diminish the responsibility of the monitoring body. This could be demonstrated with evidence that may include:
a. written contacts 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;
c. requirements relating to the termination of those contracts, in particular so as to ensure that subcontractors fulfil their data protection obligations;
and
d. the monitoring body shall ensure sufficient documented procedures to guarantee the independence, expertise and lack of conflicts of interests of the sub-contractors.

1.4 Accountability

1.4.1. 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 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).

2 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 will 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 AP with evidence that includes: personnel job descriptions, specification requirements, qualifications, required or relevant experience, published reports etc.

Requirements:

2.1 The monitoring body shall demonstrate that it has an in-depth understanding, knowledge and experience in relation to the specific data processing activities in relation to the code. Evidence as to whether it has recognised expertise may include its status as a recognised and traceable professional standards body, internal committee, trade association, interest group, federation, society or sectoral, legal, audit body or similar.

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

2.3 The monitoring body shall demonstrate that it meets the expertise requirements in 2.1 and 2.2 above and also the relevant expertise requirements as defined in the code of conduct. 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.

3 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 AP 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 expected number and size of code members. 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 and penalties as defined in the code of conduct.

Requirements:

3.1 The monitoring body shall demonstrate that they have a procedure to check prior to joining the 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.

3.2 The monitoring body shall provide evidence of upfront, ad hoc and regular procedures to monitor the compliance of members within a clear timeframe such as, procedures providing for audit plans to be carried out over a definite period and on the basis of predetermined criteria.
3.3 The monitoring body shall demonstrate that they have 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, geographical scope and complaints received.
3.4 The monitoring body shall demonstrate that their audit or review procedures define the criteria to be assessed, the type of assessment to be used and a procedure to document the findings. Review procedures can include such things as: audits, inspections, reporting and the use of self-monitoring reports or questionnaires.
3.5 The monitoring body shall demonstrate that they have 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.
3.6 The monitoring body shall be responsible for the management of all information obtained or created during the monitoring process. The monitoring body shall ensure that personnel will keep all information obtained or created during the performance of their tasks confidential, unless they are required to disclose or are exempt by law.

4 Transparent complaints handling

Explanatory note:
Transparent and publicly available procedures and structures to handle complaints in relation to code members from different sources are an essential element for code monitoring. This process will be sufficiently resourced and managed and personnel will demonstrate adequate (sufficient to the need) 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.

Where appropriate, information concerning the monitoring body's decision will be provided to all concerned within a period not exceeding three months.

Requirements:

4. Complaints about code members

4.1 The monitoring body shall provide evidence of a clear framework for a publicly available, accessible and easily understood complaints handling and decision-making process. 'This may be demonstrated for example by an outline of the procedure to receive, manage and process complaints, which in turn shall be publicly available and easily accessible.' This procedure specifies for example;
- how the complainant is informed;
- the consequences should the complaint be rejected;
- the consequences should the complaint be considered justified'

4.2 The monitoring body shall acknowledge receipt of the complaint and the complainant shall be notified on the progress or outcome of the complaint without undue delay and at the latest within three months from the receipt of the 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.
4.3 The monitoring body shall provide evidence of suitable 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.
4.4 The monitoring body shall provide evidence of their process for notifying the AP, code members and the code owner, immediately and without undue delay about the measures taken and justification of any infringements leading to code member suspension or exclusion.
4.5 The monitoring body shall maintain a record of all complaints and actions which the AP can access at any time.
4.6 In accordance with the EDPB guidelines; decisions of the monitoring body shall be made publicly available in line with its complaints handling procedure. Decisions are published when they relate to repeated and/or serious violations, such as the ones that could lead to the

suspension or exclusion of the controller or processor concerned from the code.

4.7 Otherwise publication of summaries of decisions or statistical data should be considered adequate.

5 Conflict 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.
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 any of the organisations adhering to the code. In order to avoid any conflict of interest, the personnel would declare their interest and the work would be reallocated.

Requirements:

5.1. The monitoring body shall have in place a documented procedure to identify, analyse, evaluate, treat, monitor and document on an ongoing basis any risks to impartiality arising from its activities. The monitoring body personnel shall undertake to comply with these requirements and to report any situation likely to create a conflict of interest. The monitoring body shall refrain from any action incompatible with its tasks and duties.

5.2. The monitoring body shall choose or direct and manage its personnel. This could be demonstrated by providing evidence which includes job descriptions, personnel records, recruitment personnel resource allocations and line management arrangements.
Staff can be provided by another body independent of the code. An example of staff provided by a body independent of the code would be monitoring body personnel that have been recruited by an independent external company, which provides recruitment and human resources services.

5.3. The monitoring body shall ensure that it does not seek or take instructions from any person, organisation or association and shall remain free from external influence.

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

6 Communication with the AP

Explanatory note:

The section below sets out the information the monitoring body will provide to the AP. These include 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.

Any substantial changes relating to the monitoring body's ability to function independently and effectively, its expertise and any conflict of interests could result in a review of its accreditation.

Requirements:

6.1. Applications for monitoring body accreditation with all supporting documents, as set out as examples in the requirements above, and all other correspondence must be submitted to the AP in the Dutch or the English language.

6.2. The monitoring body shall evidence a clear framework to allow for reporting of any suspensions or exclusions of code members to the AP. This reporting shall require as a minimum:
   a. inform the AP promptly and in writing of any suspension or exclusion providing valid reasons for the decision;
   b. provide information outlining details of the infringement and actions taken; and
   c. provide evidence that they have taken action in line with their suspension or exclusion process.

6.3. The monitoring body shall have a documented procedure for lifting the suspension or exclusion

of a code member and notifying that code member and the AP of the outcome of the review or investigation.

6.4. Substantial changes to the monitoring body 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.

6.5. The monitoring body shall report any substantial changes to the AP immediately and without undue delay. Substantial changes would result in a review of the accreditation.

7 Code review mechanisms

Explanatory note:

Monitoring bodies have a key role in contributing to the review of the code in conjunction with the code owner. As a result of a code review, amendments or extensions to the code may be made by the code owner.

Requirements:

7.1 The monitoring body will contribute to reviews of the code as required by the code owner and shall therefore 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 and continues to meet the application of the GDPR.
The review mechanisms should take into account any changes in the application and interpretation of the law or where there are new technological developments which have impact upon the data processing carried out by the code members or the provisions of the code.

7.2 The monitoring body shall also provide the code owner and any other establishment or institution referred to in the code of conduct with an annual report on the operation of the code. The 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.

7.3 The monitoring body shall apply code updates and implement amendments and extensions to the code as instructed by the code owner.

7.4 The monitoring body shall ensure that information concerning its monitoring functions is recorded and made available to the AP as required.

8 Legal status

Explanatory note:

The monitoring body may be set up or established in a number of different ways, for example limited companies or trade associations. 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 existence of sufficient financial and other resources should be accompanied with the necessary procedures to ensure the functioning of the code of conduct over time. The monitoring body will therefore have to provide evidence to the AP of its legal status.

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 GDPR Article 41(4).

Requirements:

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

8.2. The monitoring body shall evidence to the AP that it has the appropriate legal standing to meet the requirements of being fully accountable in its role with sufficient financial and other resources; in particular with reference to Article 83 of the GDPR and Article 14(3) of the UAVG and Article 16(1) of the UAVG, being able to take appropriate action in line with Article 41 GDPR, and that it has access to adequate resource requirements to fulfil its monitoring responsibilities. The monitoring body shall also evidence that it can deliver the code of conduct's monitoring mechanism over a suitable period of time.

Such evidence could depend on the structure of the monitoring body and could include (but not be limited to):

a. full company and business name, seat of the monitoring body and registered Chamber of Commerce number; and
b. evidence that the monitoring body has adequate financial resources to demonstrate how fines will be paid, such that the requirements of GDPR Article 83(4)(c) and Article 14(3) of the UAVG and Article 16(1) of the UAVG can be met.

8.3. 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 and therefore responsible for a fine under GDPR Article 83(4)(c) and Article 14(3) of the UAVG.

8.4. The monitoring body shall be established in the European Economic Area (EEA).

8.5. In addition to the seat of the monitoring body the names of its representatives and, if different, the names of the persons responsible for its control shall be added. Its aim is to determine who is responsible for the actions of the monitoring body and to identify the responsible department against which to take action in the event of non-compliance with its obligations.

9. Subcontractors

Explanatory note:

Monitoring bodies could engage subcontractors. The requirements below set out the relevant safeguards for engaging subcontractors.
In order to demonstrate these safeguards the monitoring body will need to provide documented evidence.

Requirements:

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

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

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.

9.4. Without prejudice to requirement 6.3, the monitoring body shall have a procedure in place to communicate to the AP 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.