Accreditation requirements for a GDPR code of conduct monitoring body

February 2024

Datatilsynet

The Norwegian Data Protection Authority

Content

Introduction

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 Conducts and Monitoring Bodies under Regulation 2016/679 (hereinafter referred to as the EDPB Guidelines), 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 Norwegian SA). 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 or an ad hoc internal committee. 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 provides 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 and follow the structure of the Guidelines.

The requirement for the Norwegian SA 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 Norwegian SA must publish these criteria.

Application Requirements

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

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 written form to the Norwegian SA. We only accept applications in Norwegian or English. The application shall contain proof of fulfilment of the requirements by submitting relevant documents, certificates etc. as set out in these requirements.

The accreditation of a monitoring body shall not be an obstacle to the development of codes of conduct. Therefore, the assessment of the application for accreditation as a monitoring body shall take into account the specificities of each sectors' processing and shall be as flexible as possible while abiding by the legal framework imposed by the GDPR, the EDPB Guidelines and the relevant Opinions of the EDPB.

The application shall, as a minimum, include the following information:

1. Information identifying the applicant, for example identification numbers such as organisation number.
2. The place of residence or registered office of the applicant, which in either case must be located in the EEA.
3. Contact information to be used for any communication in relation to the accreditation application.
4. Specification of the type of monitoring body (i.e., whether it is internal or external).
5. Specification of the code of conduct for which accreditation is being applied for.
6. The scope of the code of conduct (national or transnational).
7. Supporting documents and previous correspondence with the Norwegian SA.

Detailed documentation requirements are included in each of the accreditation requirements below.

Duration of accreditation

The Norwegian SA may review the accreditation of the monitoring body periodically according to a risk-based approach 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 indefinitely unless the outcome of a review concludes that the requirements for accreditation are no longer met. The review might result in the revocation of the accreditation of a monitoring body pursuant to Article 41 (5) GDPR.

1. Independence

The monitoring body shall be appropriately independent.

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 the monitoring of compliance with a code of conduct in complete autonomy, without being influenced directly or indirectly, nor subject to any form of pressure that might affect its decisions.

A monitoring body shall not be in a position to receive 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. Rules and procedures have to be established to ensure that the monitoring body acts autonomously and without any pressure from the code members, the profession, industry or sector to which the code applies, or from the owner of the code. When the monitoring body is internal, there must be a particular focus on the monitoring body's ability to act independently.

Independence must be demonstrated within four main areas:

- Legal and decision-making procedures
- Financial resources
- Organisational resources and structure
- Accountability

The requirements for these areas are set out below.

1.1. Legal and decision-making procedures

1.1.1. The monitoring body must be appropriately independent in relation to the code members, the profession, industry or sector to which the code applies, and the code owner itself, particularly with regard to any legal and economic link that may exist between the monitoring body and the code owner or the code members. The monitoring body must implement an appropriate decision making procedure to ensure its autonomy and independence.

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

1.1.3. The duration or expiration of the mandate of the monitoring body must be regulated in such a way 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.

1.1.4. The monitoring body shall not provide any services to code members or the code owner that can adversely affect its independence.

> **Example**
>
> Such services may be related to the development or improvement of the code of conduct, or providing guidance on the implementation of the code of conduct.

1.1.5. The monitoring body shall provide evidence during the application process that the body and its personnel can act independently and without undue pressure.

The monitoring body's independence in relation to legal and decision-making procedures may be demonstrated by:

a) Formal rules for appointment.
b) Terms of reference and job descriptions.
c) Documented recruitment processes for personnel.
d) Information on persons in the monitoring body authorised to make decisions, which shows that there are no converging interests with the entities to be monitored.
e) A description of the owners of the code.
f) Information on the duration or expiration of the monitoring body.
g) Evaluation and treatment of risks regarding independence.
h) Documents providing evidence of the business, financial, contractual, or other relations between the monitoring body and the code owners or the code members.
i) For internal monitoring bodies, a description of the operation of any committees, separate departments or personnel that may be involved with the monitoring body, and prospective information barriers between and separate reporting management structures for the organisation or body (i.e. the code owner) and the monitoring body.

1.2. Financial resources

1.2.1. The monitoring body must be appropriately financially independent. When ensuring the financial independence, the monitoring body must take into account the number and size of the code members (as monitored entities), the nature and scope of their processing activities (the subject of the code) and the risk(s) associated with the processing operation(s).

1.2.2. The monitoring body must be able to manage its budget and resources independently without any form of influence from the code owner and the code members. Internal monitoring bodies shall prove that a specific separate budget is allocated to them by the code owner.

Example

The monitoring body would not be considered financially independent if the rules governing its financial support allow a code member, who is under investigation by the monitoring body, to stop its financial contributions to it, in order to avoid a potential sanction from the monitoring body.

1.2.3. The means by which the monitoring body obtains financial support (for example, a fee paid by the members of the code of conduct) must not adversely affect its independence.

1.2.4. The monitoring body shall be able to demonstrate that it has the financial stability and resources to carry out its monitoring activities effectively and consistently, and these need to be accompanied with the necessary procedures to ensure the functioning of the code of conduct over time.

Example

This can be demonstrated with documentation of sources of income, past or projected income and expenses, and details of relevant assets or liabilities.

1.2.5. The monitoring body shall demonstrate to the Norwegian SA during the application process the means by which it obtains financial support for its monitoring role and explain how this does not compromise its independence.

1.3. Organisational resources and structure

1.3.1. The monitoring body must be organised in a way that enables it to act independently from code owners and code members within the scope of the code in performing its tasks and exercising its powers.

1.3.2. The monitoring body must have the human and technical resources necessary for the effective performance of its tasks.

1.3.3. The monitoring body must be composed of an adequate and proportionate number of personnel so that it is able to carry out the monitoring functions, reflecting the sector concerned and the nature, scope, complexity and risks of the processing activities addressed by the code of conduct.

1.3.4. The monitoring body shall be accountable and retain authority for its decisions regarding the monitoring activities. The personnel of the monitoring body can be held responsible for their activity in accordance with Norwegian law.

1.3.5. When the monitoring body is internal, there must be separate personnel and management to ensure accountability and function from other areas of the organisation (i.e. the code owner). The internal monitoring body must be able to act free from instructions and shall be protected from any sort of sanctions or interference (whether direct or indirect) as a consequence of fulfilling its task.

Example

This may be achieved by using effective organisational and information barriers and separate reporting management structures, or any other logical separation between the monitoring body and the code owners or code members.

1.3.6. The monitoring body shall demonstrate its organisational independence to the Norwegian SA during the application process.

The evidence of the monitoring body's organisational independence may be provided by

a) Identification of risks to its organisational independence and how it will remove or minimise such risks and use an appropriate mechanism for safeguarding impartiality.

b) For internal monitoring bodies, the set-up of the organisation and information concerning its relationship to its larger entity (i.e. the code owner).

1.4. Accountability

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

Example

Accountability of the monitoring body can be demonstrated by setting out a framework for the roles and decision-making framework and reporting procedures, and setting up policies to increase awareness among the personnel about the governance structures and the procedures in place.

1.4.2. 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.

1.4.3. The monitoring body must provide evidence to the Norwegian SA on its impartiality in relation to accountability during the application process.

Example

Evidence of impartiality in relation to accountability could include, but is not limited to:

a) Job descriptions.
b) Management reports and training of personnel (i.e. policies to increase awareness among the personnel about the governance structures and the procedures in place).

2. Conflict of interest

Code owners will need to demonstrate that the exercise of the monitoring body's tasks and duties does not result in a conflict of interest. As such, it must be demonstrated that the monitoring body and its personnel 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.

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.

2.1 The monitoring body must have its own personnel that are chosen by the monitoring body or some other body independent of the code. The personnel shall be subject to the exclusive direction of the monitoring body only.

> **Example**
>
> An example of personnel chosen 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

2.2 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.

2.3 The monitoring body must be protected from any sort of sanctions or interference (whether direct or indirect) by the code owner, other relevant bodies or members of the code as a consequence of the fulfilment of its tasks.

2.4 The monitoring body must identify situations that are likely to create a conflict of interest (due to its personnel, its organisation, its procedures, etc.) and provide internal procedures to deal with the effects of situations identified as being likely to create a conflict of interest. Such procedures will vary depending on the code.

> **Example**
>
> An example of a conflict of interest would be monitoring body personnel investigating complaints against the organisation that they work for. Ownership, governance, management, personnel, shared resources, finances, contracts, outsourcing, training, marketing, and payment of sales commission are other potential sources of conflict of interest.
> Example of **no** conflict of interest: Providing services which are purely administrative or organisational assistance or support activities.

2.5 In case of a conflict of interest of personnel, the personnel must declare their interests, and the work shall be reallocated.

2.6 The monitoring body shall identify and eliminate risks to its impartiality on an ongoing basis.

2.7 The monitoring body must perform awareness training of its personnel on situations likely to create a conflict of interest and the internal procedures applicable to those situations.

2.8 The monitoring body must provide information on its approach to conflicts of interest to the Norwegian SA during the application process. The monitoring body's risk management approach (as required in 2.4) and associated procedures must be included in the application.

3. Expertise

The monitoring body must have the requisite level of expertise to carry out its role in an effective manner. The requirements below aim to ensure that the monitoring body possesses adequate expertise to effectively monitor the code.

The Norwegian SA notes that all codes with monitoring bodies will need to explain the necessary expertise level for their monitoring bodies in order to deliver the code's monitoring activities effectively. The expertise of the monitoring body must be assessed in line with the particular code. Code specific requirements will be dependent on such factors as the particular sector, the processing activity, the different interests involved and the risks of the processing activities addressed by the code. These code specific requirements will be considered as part of the accreditation. The monitoring body will have to meet the requirements below in any circumstances, whereas further or specific expertise requirements will only need to be met in case that the code of conduct foresees them.

The Norwegian SA will assess the monitoring body's fulfilment of the requirements of expertise based on the monitoring body as a whole. As such, the qualifications and experience of all personnel will be included in the assessment.

3.1 The monitoring body must have an in-depth knowledge and experience in relation to data protection law as well as the sector and the particular processing activities which are the subject matter of the code.

3.2 The monitoring body must ensure 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 in the field of auditing, monitoring or quality assurance.

3.3 The monitoring body must demonstrate to the Norwegian SA during the application process that it does not only meet the requirements in 3.1 – 3.2 but also the relevant expertise requirements as defined in the code of conduct.

Evidence of the expertise of the monitoring body may include, but is not limited to:

a) Documented previous experience of the monitoring body of acting in a monitoring capacity for a particular sector.
b) Description of the competencies and previous experience of the personnel in the monitoring body.
c) Documentation of training of the personnel for carrying out the monitoring of compliance with the code.
d) Documentation related to the expertise of personnel in data protection, such as trainings and data protection certificates.

4. Established procedures and structures

The monitoring body must have an operationally feasible monitoring mechanism. The requirements below aim to ensure that the monitoring body's monitoring process is effective in terms of resources and procedures.

The Norwegian SA notes that the code itself shall define the corrective measures, and that the monitoring body must apply the corrective measures as defined in the code.

4.1 The monitoring body must be provided with the financial stability and resources necessary for the effective performance of its tasks. Resources shall be proportionate to the expected size and number of code members, as well as the complexity or degree of risk of the relevant data processing and the expected received complaints.

4.2 The monitoring body must establish procedures to assess the eligibility of controllers and processors to comply with the code. Such procedures shall include an assessment of whether the code members' processing of personal data falls within the scope of the code. In addition, the monitoring body shall provide evidence of upfront, ad hoc and regular procedures to monitor the compliance of the members within a clear time frame and check the eligibility of members prior to joining the code.

4.3 The monitoring body must establish regular procedures within a clear and defined time-period to actively and effectively monitor the code members' compliance with the code's provisions.

Example

A monitoring procedure that defines the methodology to be applied, i.e. the set of criteria to be assessed, the type of monitoring (self-assessment, off-site or on-site audits, use of recognised auditing standards etc.), the documentation of the findings, etc.

A procedure for the investigation, identification and management of infringements to the code and, when required, the corrective measures as defined by the code.

4.4 The monitoring body must establish ad hoc procedures to actively and effectively monitor the code members' compliance with the code's provisions. Ad hoc monitoring can inter alia be established on the basis of an inquiry or complaint from a data subject.

4.5 The procedures laid down in 4.3 and 4.4 and the choice between these shall be performed following a risked-based approach.

4.6 The monitoring body's monitoring procedures must address the complete monitoring processes, from the preparation of an evaluation to its conclusion, and they must include additional controls to ensure that appropriate actions are taken to remedy infringements and to prevent repeated infringements.

4.7 Procedures to monitor compliance with codes must be adequately specific to ensure a consistent application of the monitoring body's obligation.

4.8 The monitoring body must establish procedures to carry out periodic reviews of the code's operation. Further requirements regarding the code review mechanisms are set out in the requirements section 7.

4.9 When establishing the required procedures (to check for eligibility, monitoring and review), the monitoring body must take into account the risk raised by the data processing, the expected size and number of members of the code, geographical scope, complaints received and other relevant factors.

4.10 The monitoring body and its personnel are responsible for the management of all information obtained or created during the monitoring process. The monitoring body and its personnel shall keep confidential all information obtained or created during the performance of the monitoring activities, except as required by law or the requirements of this document.

4.11 Without prejudice to Norwegian legislation, the monitoring body must make decisions regarding its completed monitoring and review procedures available to the public, when they relate to repeated and/or serious violations, such as the ones that could lead to the suspension or exclusions of the controller or processor concerned from the code. Otherwise, the monitoring body must make publications or summaries of decisions or statistical data regarding its completed monitoring and review procedures available to the public.

4.12 The monitoring body must demonstrate its assessment of eligibility, monitoring and review procedures to the Norwegian SA during the application process.

5. Transparent complaints handling

Transparent and publicly available procedures and structures to handle complaints from different sources in relation to code members are an essential element for code monitoring. The requirements below aim to ensure an implementation of an effective complaints handling system.

The Norwegian SA notes that accessible complaints procedures shall be covered in the code of conduct.

5.1 The monitoring body must establish effective and clear procedures and structures for handling complaints.

> **Example**
>
> Complaint handling procedures could be a described process to receive, evaluate, track, record and resolve complaints.

5.2 In its procedures, the monitoring body must include a right of the complainant and the code member to be heard.

5.3 The monitoring body must make the complaint process publicly available and easily accessible. The guidance must be sufficiently transparent for a complainant to comprehend.

5.4 The monitoring body shall establish a timeframe for the resolution of complaints and make this information publicly available. The complaints shall be resolved within a reasonable time. If the complaint cannot be resolved within the estimated timeframe, the monitoring body must inform the complainant of the delay, the reason hereof, and of a new timeframe for the resolution of the complaint. The Norwegian SA would normally expect non-complex complaints to be resolved within three months.

5.5 The monitoring body shall acknowledge receipt of a complaint within one month.

5.6 In case of breach of a code, the monitoring body must have established procedures to take immediate action and use the corrective measures as defined in the code of conduct. The aim of such procedures must be to stop the infringement and to avoid future recurrence.

5.7 The monitoring body must be able to inform the complainant, the code member and the code owner about the measures taken and its justification without undue delay.

5.8 The monitoring body must establish procedures for the resumption of complaints.

5.9 The monitoring body must maintain a record of all complaints received and actions taken. The Norwegian SA shall have access to the record at any time.

5.10 The monitoring body must make information concerning any sanctions leading to suspension or exclusion of code members – and any subsequent lifting hereof – publicly available.

Example

Examples of sanctions: Training, issuing a warning, report to the Board of the member, a formal notice requiring the implementation of specific actions within a specified deadline, or temporary suspension of the member from the code until remedial action is taken. These measures could be publicised by the monitoring body, especially where there are serious infringements of the code.

5.11 The monitoring body must publish information about the decisions taken in the context of the complaint handling procedure. The information required may be provided in the form of general statistical information concerning the number and type of complaints/infringements and the resolutions/corrective measures issued.

5.12 The Norwegian SA has the competences to monitor the monitoring body's compliance with Article 41 (1) (2) and (4) of the GDPR pursuant to Article 57 (1) of the GDPR. As such, the monitoring body must establish procedures for informing the complainant hereof and forwarding relevant inquiries regarding the monitoring body's monitoring activity to the Norwegian SA.

5.13 The monitoring body must demonstrate its complaint handling procedures and structures to the Norwegian SA during the application process.

6. Communication with the Norwegian SA

The requirements below aim to ensure that the monitoring body's framework allows for an effective communication of actions carried out by the monitoring body in respect of the code to the Norwegian SA. This includes information concerning any suspension or exclusion of code members issued by the monitoring body and any substantial changes to the monitoring body. A substantial change will result in a review of the accreditation.

6.1 The monitoring body must set out clear reporting mechanisms to allow for reporting without undue delay of any repeated or serious infringements (which would result in severe reactions from the monitoring body, such as suspensions or exclusion from the code) to the Norwegian SA. This report shall as minimum:

a) Inform the Norwegian SA without any undue delay and in writing of the corrective measure providing valid reasons for the decision.
b) Provide information outlining details of the infringement.
c) Provide information and evidence of the actions taken.

6.2 The monitoring body must be able to provide all relevant information of any of its actions upon the request of the Norwegian SA.

6.3 The monitoring body must have a documented procedure for reviewing and lifting a suspension or exclusion of a code member and notifying the code member and the Norwegian SA of the outcome of the review.

6.4 The monitoring body must set out reporting mechanisms to allow for regular reporting of the results of the monitoring body's reviews of the code to the Norwegian SA.

6.5 The monitoring body must inform the Norwegian SA without undue delay of any substantial changes to the monitoring body.

Substantial changes may include:

a) Changes to the monitoring body's legal, commercial, ownership or organisational status and key personnel.
b) Changes to resources and locations.
c) Any changes to the basis of accreditation.
d) Any other information, which is likely to call into question its independence, expertise and the absence of any conflict of interests or to adversely affect its full operation.

6.6 The monitoring body must demonstrate its reporting mechanisms to the Norwegian SA during the application process.

7. Code review mechanisms

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.

The Norwegian SA notes that 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 must contribute to carry out reviews of the code as outlined in the code of conduct.

7.2 The monitoring body must ensure that it has documented plans and procedures to review the operation of the code.

7.3 When reviewing the code, the monitoring body must assess whether the code remains relevant to the members and continues to meet the application of the GDPR. Such an assessment shall as a minimum take into account any changes in the application and interpretation of the law and new technological developments which might have an impact upon the data processing carried out by the members or the provisions of the code.

7.4 The monitoring body shall provide the code owner and any other entity referred to in the code with an annual report on the operation of the code. The report shall include:

a) Confirmation that a review of the code has taken place and information on the monitoring body's findings and assessments following the review and whether amendments to the code are required.
b) Information concerning data breaches by code members, complaints managed and the type and outcome of monitoring functions that have taken place. This information could include, but is not limited to, general statistical information concerning the number and type of data breaches, complaints, infringements and the resolutions/corrective measures issued.
c) Confirmation that there are no substantial changes to the monitoring body.
d) Information concerning new members to the code.

7.5 The monitoring body shall apply code updates as instructed by the code owner.

7.6 The monitoring body shall ensure that information concerning its completed reviews and the annual report on the operation of the code are documented and made available to the Norwegian SA upon request.

7.7 The monitoring body shall demonstrate its review procedures to the Norwegian SA during the application process.

8. Legal status

The monitoring body can be set up or established in a number of different ways, for example as a limited company, an association, an internal department within the code owner's organisation or as a natural person. Whichever form the monitoring body takes, it must demonstrate that it has an appropriate standing to carry out its monitoring role and meet the resulting responsibilities.

The arrangements governing establishment and membership of the monitoring body, its decision-making process, operational rules and duration as well as the resources made available to it shall ensure that the monitoring body can fulfil its monitoring functions and meet the resulting responsibilities for its whole duration.

The Norwegian SA notes that a monitoring body is solely responsible for its function and tasks set out in Article 41 of the GDPR. The monitoring body is not responsible for the code members' compliance with the provisions of the GDPR.

8.1 The monitoring body must be established in the EEA.

8.2 The monitoring body must be capable of being held legally responsible for its monitoring activities. This entails that fines per Article 83 (4) (c) of the GDPR and Paragraph 26 of the Norwegian Data Protection Act ("Personopplysningsloven") can be imposed on the monitoring body and met.

8.3 During the application process, the monitoring body must demonstrate to the Norwegian SA that it is able to take appropriate action in line with Article 41 (4) of the GDPR and that it can meet the resulting responsibilities.

Evidence will depend on the structure of the monitoring body, but may include:

a) Details on the company and business, for instance in relation to the date of incorporation, the company's identification number (CVR-number), responsible officers, the number of employees, any relationships to other companies/organisations, ownership charts etc.
b) Details on relevant resources.
c) Relevant contracts, agreements, terms of references, etc.

8.4 During the application process, the monitoring body must confirm to the Norwegian SA that it is responsible for its monitoring role.

8.5 The monitoring body must demonstrate that the body is able to deliver the code of conduct's monitoring mechanism over a suitable period of time. The code of conduct itself will demonstrate that the operation of the code's monitoring mechanism is sustainable over time.

8.6 When the monitoring body is a natural person, it must be demonstrated that adequate resources are available for the natural person's specific duties and responsibilities as a monitoring body. Furthermore, it must be considered and documented how the monitoring mechanism is guaranteed over a suitable period of time and in case of a resignation or temporary inability of the person concerned. In addition, it must be demonstrated that the natural person has the necessary expertise (legal and technical).

9. Subcontracting

The monitoring body has the ultimate responsibility for decision-making and compliance when it uses subcontractors. The monitoring body can subcontract some of its activities to other parties, i.e. in relation to performing audits. 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 The decision making process cannot be sub-contracted.

9.2 Where a monitoring body uses subcontractors, the monitoring body shall ensure the effective monitoring of the services provided by the contracting entities. In addition, the monitoring body must ensure that sufficient guarantees are in place in terms of the expertise, independence, reliability and resources of the sub-contractor and that obligations applicable to the monitoring body are applicable in the same way to the subcontractor.

This can be demonstrated with evidence that may include:

a) Written contracts or agreements with the subcontractor to outline their responsibilities, including provisions on confidentiality, what type of data will be held and a requirement that the data is kept secure.
b) Clear procedures for subcontracting shall also be documented, which need to include the conditions under which this may take place, an approval process and the monitoring of subcontractors.

9.3 Where a monitoring body uses subcontractors, the monitoring body must ensure that the subcontractors comply with their data protection obligations. In addition, it shall in particular ensure the terms of termination of the contract so as to ensure that the subcontractors fulfil their data protection obligations. The contract or agreement with the subcontractor shall in particular specify the return or deletion of personal data upon termination so as to ensure that the subcontractor meets its data protection obligations, cf. Article 28 (3) (g) of the GDPR.

9.4 The monitoring body shall identify all of its subcontractors and provide information to the Norwegian SA on their tasks and the role they carry out when the monitoring body applies for accreditation. The monitoring body shall provide the same information to the Norwegian SA if the monitoring body hires a subcontractor after the accreditation. The Norwegian SA must also be informed, if the monitoring body stops using any of its subcontractors.