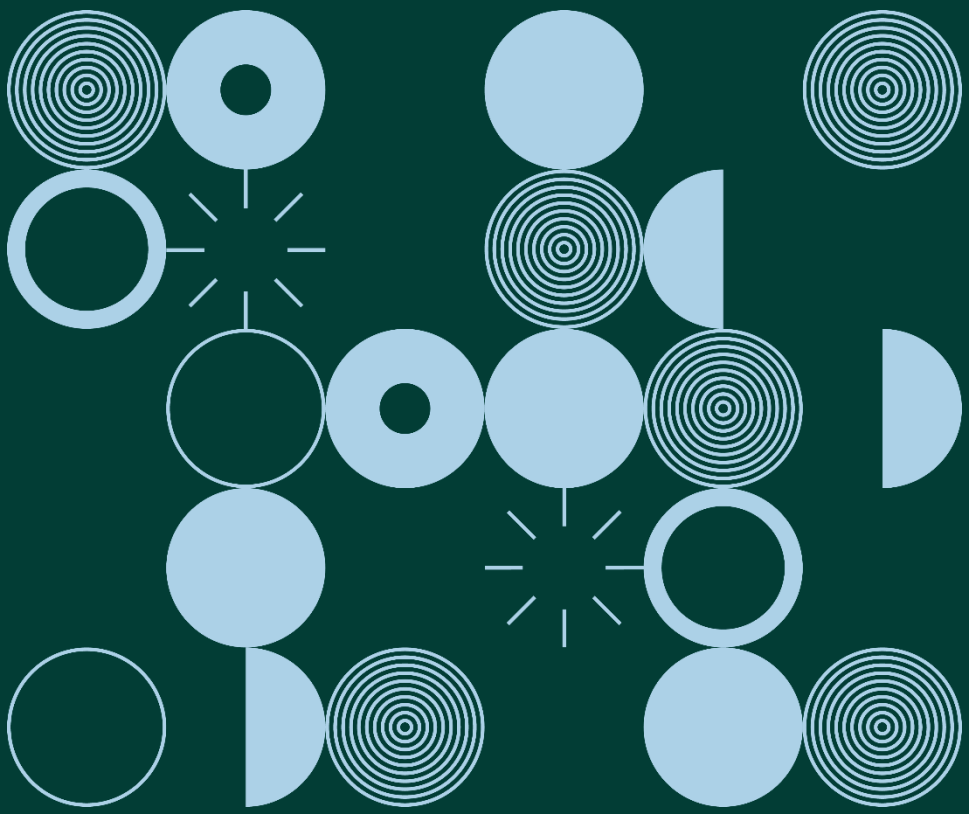
An Coimisiún um Chosaint Sonraí
Data Protection Commission

Accreditation Requirements for Code of Conduct Monitoring Bodies

December 2020



Contents

Introduction

This document sets out the requirements of the Irish Data Protection Commission (DPC) for the accreditation of monitoring bodies for Codes of Conduct ('Codes') in line with Articles 40 and 41 of the General Data Protection Regulation (GDPR). These requirements should be read in conjunction with the guidelines published by the European Data Protection Board (EDPB) on Codes of Conduct and Monitoring Bodies ('the EDPB Guidelines'),[1] and any relevant Opinions of the EDPB pursuant to Articles 41(3) and 64(1)(c) GDPR.

The Purpose of Codes of Conduct

The GDPR expressly encourages the development of voluntary compliance activities, including the drawing up of Codes aimed to contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium sized enterprises (Article 40(1) GDPR). These requirements have been drafted with the aim of working for different types of codes, applying to sectors of different sizes, and covering processing activities with different levels of risk.

Codes can be a useful and effective accountability tool, providing a detailed description of what is an appropriate, legal and, ethical set of behaviours for a particular sector or processing activity. From a data protection viewpoint, codes can therefore operate as a rulebook for controllers and processors who design and implement GDPR compliant data processing activities which give operational meaning to the principles of data protection set out in the GDPR.

Trade associations or bodies representing a sector can create codes to help their sector comply with the GDPR in an efficient and potentially cost effective way. As provided by the non-exhaustive list contained in Article 40(2) GDPR, Codes may cover topics such as (but not limited to):fair and transparent processing; legitimate interests pursued by controllers in specific contexts; the collection of personal data; the pseudonymisation of personal data; the information provided to individuals and the exercise of individuals' rights; the information provided to and the protection of children (including mechanisms for obtaining parental consent); technical and organisational measures, including data protection by design and by default and security measures; breach notifications; data transfers outside the EU; or dispute resolution procedures.

A Code must meet a particular need of a sector or processing activity, facilitate the application of the GDPR, specify the application of the GPDR, provide sufficient safeguards for data subjects, and provide effective mechanisms for monitoring

[1] EDPB, 'Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 - version adopted after public consultation', available at https://edpb.europa.eu/our-work-tools/our-documents/wytyczne/guidelines-12019-codes-conduct-and-monitoring-bodies-under_en

compliance with a code. The need for a Code monitoring body is key to fulfilling the requirement of effectively monitoring compliance with a Code.

The Need for a Monitoring Body

All Codes covering non-public authorities or bodies will be required to have a monitoring body, which have an appropriate level of expertise in relation to the subject-matter of the Code and are accredited for that purpose by the competent supervisory authority (in the case of Ireland, the DPC).

Accreditation can only be granted where the DPC is satisfied that the proposed monitoring body meets the requirements set out in Article 41 GDPR to carry out the monitoring of compliance with a proposed Code.

The GDPR and EDPB guidelines set out a broad framework for the type and structure of a monitoring body, intended to take into account the nature and context of the Code itself and thereby allow flexibility and workability for a diverse range of sectors and processing operations.

Associations or other bodies representing categories of controllers or processors which prepare Codes ('Code owners'), can put forward proposals for their Code monitoring body, in line with the requirements set out in this document, the EDPB Guidelines, and Article 41(2) GDPR. In brief, to be accredited, Code monitoring bodies must:

- ☑ Demonstrate their independence and expertise in relation to the subject matter of the Code (Article 41(2)(a) GDPR);
- ☑ Demonstrate that they have established procedures which allow them 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 (Article 41(2)(b) GDPR);
- ☑ Demonstrate that they have 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 of processor, and to make those procedures and structures transparent to data subjects and the public (Article 41(2)(c) GDPR);
- ☑ Demonstrate to the satisfaction of the DPC that the Code monitoring body's tasks and duties do not result in any conflict of interest (Article 41(2)(d) GDPR).

How to Interpret and Apply these Requirements

The DPC requests that Code owners carefully consider the requirements set out below and ensure that any Codes which are submitted to the DPC clearly address how the proposed Code monitoring body for that Code meets each of the requirements. For the

sake of clarity and efficiency, Code owners should submit this information following the headings and paragraph numbering set out in the 'Accreditation Requirements' section of this document, demonstrating how each of the numbered requirements are met, along with any supporting documentation.

Submissions should be made in either English or Irish.

The boxes below explain how explanatory notes and examples which are found throughout this document should be interpreted and applied when preparing a submission for the DPC.

Explanatory Note

Explanatory notes like this one are set out at the beginning of each of the high-level requirements, to provide a background or explanation of what is needed to satisfy the numbered sub-requirements and/or why this is needed. Nothing in the explanatory notes should be read as adding any formal requirements which are not set out in the actual text of the numbered requirements, they are merely mean to provide context and explanation.

EXAMPLES: Examples like this are set out below certain requirements, to provide a non-exhaustive sample list of the kinds of information or documents which may be provided to demonstrate compliance with the requirements set out in this document. These are merely examples, are not required in all cases, and should not be read as adding any formal requirements which are not set out in the actual text of the numbered requirements.

- Not all examples will be applicable for all Codes (reflecting the diverse range of possible Codes and monitoring bodies).
- Types of information or documentation not mentioned in these examples may also be appropriate or necessary, depending on the context.

The proposed introduction of any new or additional monitoring body for a Code will require the new proposed body to also be assessed in line with the accreditation criteria contained in this document.

Accreditation Requirements

The following are the requirements which the proposed monitoring bodies for any Codes submitted to the DPC must meet in order to be accredited. The Code owners making a submission to the DPC must satisfactorily demonstrate that each of these requirements is met in order for the monitoring body to be accredited.

Requirements listed below should be understood to apply to all forms of monitoring bodies, both external and internal, unless otherwise indicated.

1. Independence

Explanatory Note

Article 41(2)(a) GDPR requires that a monitoring body must have 'demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority'.

The requirements set out below set out what must be demonstrated to satisfy the DPC that a proposed monitoring body has the requisite independence to carry out its monitoring role, under the sub-headings of 'Structure, Power, and Functions' as well as 'Budget and Resources'.

A monitoring body must have an appropriate structure as well as rules and procedures to ensure that it can carry out its monitoring task impartially and without influence from the members of the Code and/or the Code owner, and the sector, profession, or industry to which the Code is intended to apply. This includes being able to demonstrate how they will maintain sufficient resources to ensure the functioning of the Code over time.

A monitoring body can be either *internal* or *external* with regards to the Code owner, once it can be demonstrated that its structure and procedures are adequate to demonstrate its independence. Examples of internal monitoring bodies could include an *ad hoc* internal committee or a separate, independent department within the Code owner. It will be for the code owners to explain the risk management approach with regard to its impartiality and independence. Internal monitoring bodies in particular will need to provide evidence that its independence or impartiality is not compromised by any undue influence or pressure from the Code members and/or Code owner.

Requirements:

1.1 Structure, Powers, and Functions

1.1.1 The monitoring body shall be appropriately independent in relation to the Code members, the profession, industry or sector to which the Code applies and in relation to the Code owner itself.

1.1.2 An *internal* monitoring body shall provide information concerning its relationship to its larger entity (for example, the Code owner) and shall evidence its independence from any larger entity it is a part of or associated with.

EXAMPLES: This could be demonstrated by information barriers between the monitoring body and its larger entity/the Code owner, separate reporting structures, separate operational and

personnel management functions, and/or by using different logos or names, as appropriate. Evidence should suffice to demonstrate that the monitoring body is able to act free from instructions and is protected from any sort of sanctions or interference as a consequence of the fulfilment of its task.

1.1.3 The monitoring body shall retain the authority and responsibility and act independently regarding its choice and application of its monitoring activities, including sanctions.

1.1.4 The monitoring body shall be able to demonstrate that any personnel and/or committees involved in decision-making are free from any commercial, financial, or other pressures that might influence decisions, and that they can act independently, in particular in relation to:

a) supervision of resources and finances of the monitoring body;

b) decisions on and performance of compliance monitoring; and

c) the safeguarding of the impartiality of the monitoring body.

EXAMPLES: The above (1.1.3-1.1.4) could be demonstrated by formal rules for appointment, remuneration arrangements, personnel or committee mandates or terms of reference, or other documentation of the powers, voting rights, and operation of any personnel and/or committees that may be involved with decision-making within the monitoring body.

1.2 Budget and Resources

1.2.1 The monitoring body shall be able to demonstrate, on an ongoing basis, that it has the financial stability and resources to effectively and consistently carry out its monitoring

EXAMPLES: This could be demonstrated by documentation of sources of income, past or projected income and expenses, and details of relevant assets or liabilities.

activities.

1.2.2 The monitoring body shall be able to manage its budget and resources independently and effectively monitor compliance without any form of influence from the Code owner or Code members.

1.2.3 The monitoring body shall be able to demonstrate to the DPC the means by which it obtains financial support for its monitoring role and demonstrate how this does not compromise its independence.

EXAMPLES: The above (1.2.2-1.2.3) could be demonstrated by rules or procedures regarding funding, such as through financial contributions by Code members, and safeguards in place to ensure that undue pressure cannot be put on the monitoring body by the risk or threat of funding being revoked, particularly by a Code member under investigation or sanction.

1.2.4 The monitoring body shall have adequate resources and staffing necessary to effectively perform its tasks, in particular that the monitoring body has proportionate and sufficient resources and numbers of sufficiently qualified personnel to carry out its monitoring function, taking into account the sector and processing activities covered by the Code.

EXAMPLES: Evidence that personnel are sufficiently qualified could include details of legal, technical, and/or administrative experience and qualifications, as appropriate to the context of the Code, in particular the nature of any qualifications, how recent they are, and any continuing professional development obligations.

In demonstrating the adequacy of the monitoring body's resources and personnel, evidence provided could include the expected number and size of Code members, as well as the complexity or degree of risk of the relevant data processing operations involved.

1.2.5 Where a monitoring body uses sub-contractors, it shall ensure that sufficient guarantees are in place in terms of the knowledge, reliability, and resources of the sub-contractor and obligations applicable to the monitoring body are applicable in the same way to the sub-contractor. The use of subcontractors does not remove the responsibility of the monitoring body, which remains ultimately responsible for compliance with its obligations as a monitoring body, notwithstanding the sub-contractor's responsibility and obligations.

1.2.6 Where a monitoring body uses sub-contractors, it shall ensure effective monitoring of the services provided by the contracting entity.

EXAMPLES: The above (1.2.5-1.2.6) could be demonstrated by (a) written contacts or agreements outlining responsibilities, as well as confidentiality and data protection obligations; (b) clear procedures for sub-contracting, including the conditions under which this may take place, approval processes, and monitoring of subcontractors; or (c) documented procedures to guarantee the independence, expertise, and lack of conflicts of interest regarding sub-contractors.

1.3 Accountability

1.3.1 The monitoring body shall be able to demonstrate that it is accountable for its decisions and actions.

EXAMPLES: This could be demonstrated by, for example, setting out a framework for its roles and reporting procedures and its decision-making process to ensure independence. 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).

1.3.2 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.

2. Conflicts of Interest

Explanatory Note

Article 41(2)(d) GDPR requires that a monitoring body must have 'demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests'.

Code owners need to 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 in incompatible activities. Similarly, the monitoring body must remain free from external influence, whether direct or indirect, which could lead to or constitute a conflict of interest. These requirements are closely related to the requirements above regarding 'Independence'.

Risk regarding impartiality and conflicts of interest may arise in relation to ownership, governance, management, staffing, shared resources, finances, contracts, outsourcing, training, marketing, or a representative role of a parent entity for internal monitoring bodies.

Requirements:

2.1 The monitoring body shall not provide any services to or engage in any other activities vis-à-vis Code members or the Code owner, that would adversely affect its impartiality or present a conflict of interest, and must be able to demonstrate how they have managed their activities in such a manner to mitigate any actual or potential sources of conflict of interest arising out of such services or activities.

EXAMPLES: This could be demonstrated by an assessment of potential conflicts or risks to impartiality in the context of services provided, and how these were rated or mitigated. Certain situations, particularly relevant in the case of internal monitoring bodies, which may not result in a conflict of interest could include, among others, services, which are purely administrative or organisational assistance or support activities, which have no influence on the impartiality of the monitoring body.

2.2 The monitoring body shall have a process to identify, analyse, evaluate, treat, monitor and document on an ongoing basis any risks to impartiality or conflict of interests 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.

EXAMPLES: This could be demonstrated by a documented and systematic assessment of potential risks to impartiality or conflicts of interest, and how these were are mitigated or eliminated, as well as procedures and training for personnel to ensure conflicts are detected and reported.

2.3 The monitoring body shall choose or direct and manage its own personnel (or have personnel provided by a body independent of the Code, Code owner, or members).

EXAMPLES: This could be demonstrated by job descriptions, personnel records, details of recruitment processes, personnel resource allocations, and line management arrangements. A

body independent of the Code could include an independent external company, which provides recruitment and human resources services.

2.4 The monitoring body shall ensure that it does not seek or take instructions from any person, organisation, or association with regard to the carrying out of its monitoring functions and shall remain free from external influence.

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

3. Expertise

Explanatory Note

Article 41(2)(a) GDPR requires that a monitoring body must have 'demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority'.

The aim of the requirements below is to ensure that the monitoring body possesses adequate competencies and expertise to undertake effective monitoring of the Code, by providing 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 covered by the 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.

Requirements:

3.1 The monitoring body shall have an appropriate level of experience and expertise in data protection with regards to the issues and processing activities which are the subject matter of the Code, taking into account in particular the processing operations and sector involved.

EXAMPLES: This could be demonstrated by experience in data protection and/or monitoring and promoting compliance with data protection obligations, and appropriate experience, training, and qualifications of personnel of the monitoring body.

3.2 The monitoring body shall have an in-depth understanding, knowledge and experience in relation to the specific sector and/or data processing activities which are the subject matter of the Code.

EXAMPLES: This could be demonstrated by previous work, published reports, or status as a recognised experienced professional standards body, internal committee, trade association, interest group, federation, society, audit body, or similar entity.

3.3 The monitoring body shall demonstrate that its relevant personnel have appropriate data protection expertise and operational experience, training, and qualifications.

EXAMPLES: This could be demonstrated by previous experience in auditing, compliance, quality assurance, and monitoring, and the level of experience, training, and qualifications (including that required at the recruitment stage) of relevant personnel (such as those involved in monitoring, audits, or decision-making), as well as details of any training conducted, facilitated, or planned.

3.4 The monitoring body shall meet any additional specific expertise requirements which arise from the Code itself or the subject matter of the Code, where applicable, specifically

regarding the expertise required to effectively monitor in the context of the sector and/or processing activities which the Code covers.

4. Established Procedures and Structures

Explanatory Note

Article 41(2)(b) GDPR requires that a monitoring body must have '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'.

These requirements aims to ensure that monitoring bodies have a comprehensive assessment procedure which adequately assess the eligibility of controllers and processors to sign up to and comply with the Code. It should also ensure that the provisions of the Code are capable of being met by the controllers and processors.

Monitoring bodies must also have procedures and structures in place which allow them to actively and effectively monitor compliance by members of the Code on an ongoing basis, and to carry out periodic reviews of the code's operation. Monitoring bodies should consider the publication of audit reports as well as the findings of periodic reporting from controllers and processors within the scope of the Code.

The appropriate timeline for 'periodic' review and monitoring activities will depend on factors such the nature of the Code, the processing activities, and the Code member(s) concerned, and should be appropriate given the complexity and risks involved. The procedures for triggering *ad hoc* review or monitoring activities should similarly be informed by the circumstances of the Code and be appropriate to the complexity and risks involved.

Requirements:

4.1 The monitoring body shall be able to demonstrate that it has a procedure to assess eligibility of prospective members to comply with the Code, and that they are capable of meeting the provisions of the Code.

EXAMPLES: This could be demonstrated by application and assessment procedures and requirements for members to join the Code, including assessment of whether a prospective member's processing of personal data falls within the scope of the relevant Code and whether their current operations satisfy the requirements of the Code.

4.2 The monitoring body shall have established procedures for monitoring compliance of Code members with the Code, taking into account considerations such as the complexity and risks involved in the sector and processing activities which are the subject of the Code, the number of Code members, the sectoral or geographical scope, and the number and nature of complaints to be handled.

4.3 The monitoring body shall have established procedures for periodic review of the operation of the Code, including assessment of any required updates to the content of the Code or arrangements regarding membership thereof, taking into account considerations such as the complexity and risks involved in the sector and processing activities which are the subject of the Code, the number of Code members, the sectoral or geographical scope, and the number and nature of complaints to be handled.

EXAMPLES: The above (4.2-4.3) could be demonstrated by procedures and structures such as random or unannounced audits, annual inspections, regular reporting, and the use of questionnaires, as well as feedback and review mechanisms for the Code itself.

4.4 The monitoring body shall have established audit or review procedures which define the criteria to be assessed, the type of assessment to be used, and a procedure to document the findings, and ensure those procedures and structures are transparent to data subjects and the public.

EXAMPLES: This could be demonstrated by written procedures regarding audits, inspections, reporting, etc., and details of how these are made available to Code members, concerned data subjects, and members of the public.

4.5 The monitoring body shall have demonstrated procedures 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.

EXAMPLES: This could be demonstrated by procedures for the monitoring body to impose corrective measures such as suspension or exclusion of the infringing Member from the Code.

4.6 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.

5. Transparent Monitoring Procedure

Explanatory Note

Article 41(2)(c) GDPR requires that a monitoring body must have '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'.

The aim of this requirement is to ensure that a monitoring body has an effective, publicly accessible complaints-handling process which is sufficiently resourced and structures which can deal with handling complaints in an impartial and transparent manner, ensuring that decisions of the body are made publicly available. This requirement also aims to ensure that relevant information on the monitoring body's other monitoring activities (apart from formal decisions regarding suspension or exclusion) is made available.

Requirements:

5.1 Monitoring of and Complaints about Code Members

5.1.1 The monitoring body shall also have in place a procedure for ensuring the Code itself is publicly available.

5.1.2 The monitoring body shall have clear framework for a publicly available, accessible, and easily understood complaints-handling process for complaints against Code members.

EXAMPLES: This could be demonstrated by an established process to receive, evaluate, track, record, and resolve complaints, which would be outlined in publicly available guidance for the Code so that a complainant can understand and follow the complaints process. This could include detail on the range of outcomes and escalation procedures for complaints or infringements of differing levels of severity.

5.1.3 The monitoring body shall acknowledge receipt of the complaint without undue delay and provide the complainant with a progress report on or a final outcome to their complaint within a reasonable time period, at the latest within 3 months from receipt of the complaint.

5.1.4 The monitoring body shall have suitable corrective measures available to it, determined in the Code, in cases of infringement of the Code by a Code member, to stop the infringement and avoid future re-occurrence.

EXAMPLES: This could be demonstrated by details of available corrective measures such as training, issuing a warning, report the member to the board, formal notice requiring remedial action, temporary suspension or definitive exclusion from the code, as well as details of how these can be applied to and enforced against Code members.

5.1.5 The monitoring body shall have a suitable process for notifying the DPC without undue delay about any corrective measures taken and justification of any decision leading to Code member suspension or exclusion for infringement of the Code.

5.1.6 The monitoring body shall have a documented procedure for maintaining a record of all complaints and actions, which the DPC can access at any time.

5.1.7 The monitoring body shall have a documented procedure for providing publicly available information, at regular intervals, about its monitoring activity, in accordance with the Code and its complaints handling procedure, which shall include at a minimum information on any sanctions leading to suspension or exclusion of Code members from the Code.

EXAMPLES: This could be demonstrated by a demonstrated procedure for statistics on monitoring and/or audit activities, complaints received, types of infringements, and applied corrective powers, and/or publishing details or summaries of actions taken, or including relevant information in a public annual report.

5.2 Complaints about the Monitoring Body

5.2.1 The monitoring body shall have clear framework for a publicly available, accessible, and easily understood complaints-handling process in relation to complaints made against it, including appeals in relation to its decisions.

EXAMPLES: This could be demonstrated by an established process to receive, evaluate, track, record, and resolve complaints or appeals, which would be outlined in publicly available guidance for the Code so that a complainant can understand and follow the process.

5.2.2 The handling process for complaints against the monitoring body or appeals against its decisions shall include at least the following:

a) a description of the process for receiving, validating, investigating the complaint or appeal and deciding what actions are to be taken in response to it;

b) tracking and recording complaints and appeals, including actions taken to resolve them; and

c) ensuring that any appropriate action is taken in a timely manner.

5.2.3 The monitoring body shall acknowledge receipt of the complaint without undue delay and provide the complainant with a progress report on or a final outcome to their complaint within a reasonable time period, at the latest within 3 months from receipt of the complaint.

5.2.4 The monitoring body shall assist in the investigation and resolution of any complaints made about the monitoring body to the DPC.

6. Communication with the Data Protection Commission

Explanatory Note

A proposed framework for any monitoring body needs to allow for the effective communication of monitoring activity carried out by the monitoring body in respect of monitoring of compliance with the Code to the DPC. This could include decisions concerning the actions taken in cases of infringement of the Code by a Code member, providing periodic reports on the code, or providing review or audit findings of the code.

The proposed monitoring body will also need to have a procedure in place to inform the DPC of any substantial changes to its circumstances, which could influence its ability to conduct its role of monitoring the Code. Substantial changes to the circumstances of the monitoring body would result in a review and could result in a revocation of accreditation by the DPC.

The appropriate regularity and level of detail to be included in communications with the DPC should be proportionate to the nature and seriousness of the issues involved, with more significant issues proactively communicated on an ad hoc or regular basis and more general monitoring activity communicated by way of overviews in periodic reporting (such as through the annual monitoring report, or more regular overviews or status reporting). Not every monitoring action undertaken by the monitoring body will need to be individually communicated to the DPC.

Requirements:

6.1 The monitoring body shall have a clear framework for reporting any suspensions or exclusions of Code members from the Code to the DPC. This reporting framework shall require as a minimum that the monitoring body will:

- **a)** inform the DPC without undue delay and in writing of any suspension or exclusion of a Code member, providing reasons for the decision;
- **b)** provide sufficient information outlining details of the infringement and actions taken; and
- **c)** provide evidence that it has taken commensurate action in accordance with its suspension or exclusion process as outlined in the Code.

6.2 The monitoring body shall have a documented procedure notifying the affected Code member and the DPC of the outcome of any audit, review, or investigation of a Code member's compliance with the Code or of any review of previously exercised exclusions or suspension from the Code, with a level of detail and regularity appropriate to the circumstances.

EXAMPLES: This could be demonstrated by a process for documenting audits, reviews, or investigation, such as through reports, containing details such as the date of the audit, its scope, the identity of the auditee, the audit conclusion, and if corrective were exercised. Depending on the circumstances, such as seriousness of suspected or identified non-compliance with the Code, this information could be provided at regular intervals such as monthly, quarterly, or annual reports, as appropriate. Further, such documentation should be available to the DPC on request.

6.3 The monitoring body shall have a documented procedure for notifying the DPC of any complaints made against it which are upheld, including appeals in relation to its decisions, as set out in requirement 5.2, with a level of detail and regularity appropriate to the circumstances.

6.4 The monitoring body shall have a documented procedure for notifying the DPC of any substantial changes to the circumstances, structure, or processes of the monitoring body with a level of detail and regularity appropriate to the circumstances.

EXAMPLES: Substantial changes to the monitoring body may include but are not limited to changes regarding: its legal, commercial, ownership or organisational status and key personnel; resources and location(s); and any changes to the basis of accreditation.

6.5 The monitoring body shall have a documented procedure for notifying the DPC, without undue delay, of any significant concerns regarding the operation of the Code arising from their monitoring activities pursuant to requirements 4.1 – 4.3 which is likely to result in a high risk to the data protection rights of affected data subjects.

6.6 The monitoring body shall have a documented procedure for providing an annual monitoring report on the operation of the Code to the DPC, as well as to the Code owner and/or entity nominated in the Code. The annual monitoring report shall include at least at statement of assurance of compliance with these accreditation requirements, a summary of monitoring activity, as well as details on:

a) the membership of the Code;
b) members who have joined, or been suspended or expelled from the Code;
c) the number of complaints received against Code members and against the monitoring body and the outcomes thereof;
d) the number and nature of any corrective powers exercised;
e) the findings of any review of the Code, as per requirement 7 'Review Mechanisms'.

EXAMPLES: The annual report could include details such as the number of audits, reviews, investigations or other monitoring activities engaged in during the year, the number and nature of complaints received, the number and nature of any corrective powers exercised, and any operational issues encountered and recommendations for updates to the Code, as well as any other relevant information or observations regarding the functioning of the Code and the monitoring activities of the Code monitoring body.

6.7 The monitoring body shall maintain records concerning the carrying out of its monitoring functions, and make them available to the DPC as required.

7. Review Mechanisms

Explanatory Note

Article 41(2)(b) GDPR requires that a monitoring body must have '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'.

Monitoring bodies thus have a key role in contributing to the review of the Code in conjunction with the Code owner, who is ultimately responsible for the updating of the Code. As a result of a Code review, amendments or extensions to the Code may be made by the Code owner.

Review mechanisms should be put in place 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 relevant data processing operations within the scope of the Code.

Requirements:

7.1 The monitoring body shall have documented plans and procedures to review the operation of the Code, in the context of its compliance-monitoring function, and to share its feedback to the Code owner or any other relevant entity

EXAMPLES: This could be demonstrated by documented procedures for informing the Code owner of operational challenges to monitoring the Code, or to common compliance issues noted by the monitoring body in carrying out its monitoring function.

7.2 The monitoring body shall have documented plans and procedures to contribute to any review or revision of the Code itself by the Code owner to ensure that the Code remains relevant to the members and continues to meet the application of the GDPR.

7.3 The monitoring body shall apply and implement updates, amendments, and/or extensions to the Code, as decided by the Code owner.

8. Legal Status

Explanatory Note

The monitoring body may be set up or established in a number of different ways, for example limited companies, trade associations, representative groups or societies. It may be either separate from the Code owner (external) or a distinct and independent part of the Code owner (internal). Whatever form the monitoring body takes, it must demonstrate sufficient financial and other resources to deliver its specific duties and responsibilities.

The monitoring body will therefore have to provide evidence to the DPC of its legal status including, where practical, the names of owners or named responsible officers and, if different, the names of the persons who control it. Further, and linked to the requirements regarding independence and conflicts of interest, the monitoring body will have to show that it has the necessary structure(s) and procedures to ensure its long-term financing and viability.

The proposed monitoring body (whether internal or external) and related governance structures will need to be formulated in such a manner whereby the code owners can demonstrate that the monitoring body has the appropriate standing to carry out its role under Article 41(4) and is capable of being fined as per Article 83(4)(c) GDPR. This requirement requires that the monitoring body is legally capable of being fined, rather than necessitating that the monitoring body show it has sufficient funds to cover such a fine. 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. However, a monitoring body is not responsible for Code members' GDPR compliance.

Requirements:

8.1 The monitoring body shall have the appropriate legal standing to meet the requirements of being fully accountable in its role and to fulfil its monitoring responsibilities.

8.2 The monitoring body, in particular, shall have adequate legal standing to ensure that fines per Article 83(4)(c) GDPR can be imposed and met.

EXAMPLES: The above could be demonstrated by full company and business name and date and place of incorporation, memorandum and articles of association, details of shareholders and directors, registered office and number, ownership chart, details of interests in or relationship to any other entity.

Details should also be provided such as evidence of appropriate legal powers and resources for the monitoring body, any relevant resolutions of the relevant shareholders or boards of directors (or equivalent for unincorporated associations or trade associations or similar), any relevant contracts, undertakings, membership requirements, guarantees, formal agreements, terms of reference and appointment, and decision making procedures.

8.3 The DPC shall be provided with information on the legal relationship, if any, between the proposed monitoring body and the Code owner, and details as to how this does not adversely impact the carrying out of its monitoring functions.

8.4 The monitoring body shall have an establishment in the EEA.

An Coimisiún um Chosaint Sonraí
Data Protection Commission

An Coimisiún um Chosaint Sonraí
21 Cearnóg Mhic Liam, BÁC 2,
DO2 RD28, Éireann

Data Protection Commission
21 Fitzwilliam Square, Dublin 2,
D02 RD28, Ireland