Accreditation Requirements for Monitoring Bodies

Information and Data Protection Commissioner
Published on 17 January 2023

CONTENTS Page

1. INTRODUCTION

The General Data Protection Regulation[1] (the "**GDPR**" or the "**Regulation**") stipulates that Member States, supervisory authorities, the European Data Protection Board (the "**Board**") and the European Commission shall encourage the drawing-up of codes of conduct intended to contribute to the proper application of the Regulation, taking into account the peculiarity of the specific industries and the needs of micro, small and medium-sized enterprises. The main purpose of codes of conduct is to translate generic data protection obligations into more sector-specific, voluntary rules to be followed by controllers and processors that operate in a particular industry (the "**code members**"). This is aimed at facilitating compliance with data protection law by code members which, by adhering to a code of conduct, commit to abide by a digestible set of rules which takes into account the peculiarity and challenges of the sector concerned. Codes of conduct may be prepared by an association and / or another body representing categories of code members, referred as code owner (the "**code owner**"[2]). As a mandatory requirement, compliance with a code of conduct by code members must be monitored by an external or internal body having an appropriate level of expertise in relation to the subject-matter of the code. This entity is referred to as the monitoring body (the "**monitoring body**"[3]). The capacity of a monitoring body to effectively monitor a code of conduct is assessed by the competent supervisory authority in the context of a formal accreditation process (the "**accreditation**"[4]). This document lays down the accreditation requirements to be fulfilled by a monitoring body insofar as the Office of the Information and Data Protection Commissioner of Malta (the "**IDPC**") acts as the competent supervisory authority. The requirements laid down within this document must have been attained by the monitoring body prior to the submission of an application for accreditation and must by maintained for the entire duration of the monitoring function. Should any of these requirements not have been fulfilled prior to the application, the monitoring body shall duly explain how such requirement will be met, and which actions are planned in that regard. An accredited monitoring body must report to the supervisory authority without undue delay any supervening event that may undermine its capacity to conduct its operations, or that may cause full or partial loss of any of the statutory requirements for accreditation.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
[2] In this document, "accreditation" shall have the same meaning as in section 2 of EDPB Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, Version 2.0, 4 June 2019 (the "**Guidelines**").
[3] Ibid.
[4] Ibid.

2. ACCREDITATION REQUIREMENTS

Article 41 (2) of the GDPR contains a list of requirements which the proposed monitoring body must meet in order to gain accreditation. At the same time, the Guidelines provide practical guidance and interpretative assistance in relation to the application of Articles 40 and 41 of the GDPR. A body that intends to apply for accreditation must demonstrate to be in possession of the requirements laid down in this document at the time of the application. The application for accreditation, as well as any information annexed to the application, shall be in writing and shall be drafted in the Maltese or in the English language. It is remarked that it is not necessary to accredit a monitoring body if a code of conduct only applies to public authorities and bodies. Nonetheless, the implementation of effective mechanisms to monitor the code, such as audit requirements or other forms of structured monitoring, shall still be in place. 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.

3. LEGAL STATUS

The code of conduct itself needs to demonstrate that the operation of the code's monitoring mechanism is sustainable over time and covering worst-case scenarios, such as the monitoring body being unable to perform the monitoring function. A monitoring body shall demonstrate that it can deliver the code of conduct's monitoring mechanism over a suitable period of time.

3. 1 TYPE OF ENTITY

The monitoring body shall comprise of either a legal or a natural person, for-profit or not-for-profit, which must be established in the EEA[5]. The monitoring body may be external or internal. The requirements indicated herein shall apply to both external and internal proposed monitoring bodies, unless specified otherwise[6]. An internal monitoring body may include a committee or a separate and independent department within the code owner; however, this may not be set up within a code member. The internal or external monitoring body shall remain responsible to demonstrate compliance with these accreditation requirements and to maintain such requirements for the entire duration of the monitoring function. The monitoring body must ensure that these requirements are fulfilled in an impartial and independent manner, and without any influence.

[5] European Economic Area, as established in the Agreement on the European Economic Area.
[6] Infra, section 4.1, first paragraph, letter (x); section 4.1, second paragraph, letters (i) to (vii); section 4.3, first paragraph, letter (iii); section 4.3 third paragraph, letters (i) to (iv); section 4.4, page 11; section 5, page 12.

3. 2 STANDING

The monitoring body shall demonstrate that it has appropriate standing to carry out its functions under Article 41(4) of the GDPR. In this respect, the monitoring body:

i.	shall have the legal capacity to sue and be sued;
ii.	shall have the legal capability of being fined;
iii.	shall be accountable under Article 5(2) and Article 24 of the GDPR and shall be subject to the enforcement action of supervisory authorities, which may include administrative fines, in case it fails to deliver its monitoring functions and to take appropriate action when code requirements are infringed; and
iv.	shall fulfil the requirements of financial standing, professional competence and shall have a decision-making procedure in place which describes the roles of all parties in order to shield the monitoring body from any influence.

The monitoring body shall exhibit compliance with the above requirements by providing evidence thereof. Such evidence, which depends on the structure and legal nature of the monitoring body, shall include, without limitations:

i.	documents certifying the full legal name, type of entity, registered address, registration number, date of formation, names of executive officers, certificates of incorporation and of good-standing; and
ii.	evidence that the monitoring body has adequate financial resources to demonstrate how administrative fines would be paid, so that the requirements of Article 83(4)(c) of the GDPR can be met.

3. 3 ACCESS TO RESOURCES

The monitoring body has access to the necessary resources thus to fulfil its role and to deliver the code owner's monitoring mechanism in a timely and efficient manner. In addition, the monitoring body shall be equipped with adequate work force and with technical and logistical assets to further strengthen its monitoring responsibilities. These resources shall enable the monitoring body to perform its responsibilities in a complete and autonomous manner whilst remaining independent, impartial and free from any influence by the code owners and by the code members. Furthermore, the monitoring body shall demonstrate to have and to maintain over time the necessary financial means to operate and to meet its day-to-day running, whilst properly budgeting and planning such resources. The monitoring body shall be in a position to furnish evidence of the source of its financial

means. Financial stability and access to resources need to be accompanied with the necessary procedures to ensure the functioning of the code of conduct over time.

3. 4 USE OF SUB-CONTRACTORS

The monitoring body may farm out certain monitoring activities, which shall not include the decision-making process, to other entities acting as sub-contractors. When doing so, the monitoring body must ensure to implement the appropriate safeguards to ensure that the appointed sub-contractors have a sufficient level of expertise, trustworthiness and accountability. The monitoring body shall remain responsible for compliance when it uses sub-contractors. On the other hand, sub-contractors which are engaged by the monitoring body are required to comply with their data protection obligations. When engaging a sub-contractor, the monitoring body shall make certain that:

i.	ultimate responsibilities that pertain to the monitoring body are not in any manner shifted to a sub-contractor, and that the monitoring body remains liable towards all stakeholders in lieu of the sub-contractor;
ii.	the sub-contractor conforms to the same requirements which apply to the monitoring body, which include but are not limited to financial standing, professional competence and shall have a decision-making procedure in place which describes the roles of all parties in order to shield the monitoring body from any influence;
iii.	the relationship between the monitoring body and the sub-contractors is governed by a legally-binding and enforceable written agreement, which clearly stipulates the subject-matter, duration, nature and purpose of engagement, what personal data and which categories of data subjects are involved and disciplines the obligations and rights of the monitoring body to process the personal data in a secure manner. The agreement shall include provisions concerning the consequences of its termination, which shall bind the sub-contractor to fulfil its related data protection obligations;
iv.	it follows formally documented procedures to engage a sub-contractor, which regulate the tasks which are being sub-contracted, the conditions under which this may take place (i.e. independence, expertise and lack of conflicts), the approval process and the monitoring of sub-contractors; and
v.	documented procedures that establish the actions to be taken in case of conflict of interest between the monitoring body and the sub-contractors are in place.

4. INDEPENDENCE

The monitoring body must provide for and demonstrate impartiality of functions from the code members and profession, industry or sector to which code applies in a manner that ensures its independence. This shall be achieved by establishing a series of formal rules and procedures for the

appointment, terms of reference and operation of the monitoring body. These rules and procedures shall ensure the complete autonomy of the monitoring body from any direct or indirect influence or pressure at any time. The independence of the monitoring body, which shall be upheld at any time, and not only during the decision-making process, shall be demonstrated in four areas, as detailed below:

i.	legal and decision-making procedures;
ii.	financial;
iii.	organisational, and
iv.	accountability.

4.1 LEGAL AND DECISION-MAKING PROCEDURES

The legal structure of the monitoring body, including its ownership, and its decision-making procedures must shield the monitoring body from any external or internal influence. The independence and impartiality of such decision-making procedures shall be demonstrated by submitting relevant documents, which may include, without limitations:

i.	articles of incorporation of the monitoring body and articles of incorporation of the code owner;
ii.	organigram of the monitoring body and of the code owner;
iii.	description of the decision-making process which indicates the roles and prerogatives of all parties involved in such process;
iv.	formal rules for appointment and documented recruitment processes for the personnel of the monitoring body;
v.	independence in the designation of its personnel;
vi.	evidence that the decision-making personnel of the monitoring body has no convergent interests with the entities subject to monitoring. In this regard, the monitoring body must bring information concerning the activities (gainful or not) in which such personnel is engaged;
vii.	exposure over the beneficial owners[7] of the monitoring body;
viii.	information on the duration or expiration of the monitoring body's functions. 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. For example, tying the renewal of the mandate to the enforcement actions taken by the monitoring body over a period of time is not acceptable.

[7] "beneficial owner" shall have the same meaning as in article 3(6) of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015.

ix.	evaluation and treatment of the risk to the monitoring body's independence; and / or
x.	in the case of an internal monitoring body, detailed description of all operations of any committees, separate department or personnel that may be involved with the monitoring body.

In case the monitoring body is internal, it is mandatory that the impartiality of the relationship with the pertaining entity (e.g. the code owner) is preserved. Hence, the internal monitoring body is bound to demonstrate that certain measures, such as those listed down below, have been implemented:

i.	information barriers;
ii.	separate reporting and separate operational structures;
iii.	segregation of management functions;
iv.	separate staff and management;
v.	separate accountability and function from other areas of the organisation; and
vi.	that the monitoring body is 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 the fulfilment of its tasks.

In order to protect its integrity, the monitoring body must not provide any service to the code owner and to code members which would adversely affect its independence. Nevertheless, the provision of services which are purely administrative or organisational assistance or support activities by the monitoring body to the code owner and / or to the code members is not likely to constitute a conflict of interest[8]. Furthermore, any decision made by the monitoring body shall not be subject to approval by any other organisation, including the code owner. Thus, no type of interference shall affect the monitoring body's independent decision-making process.

4.2 FINANCIAL INDEPENDENCE

The monitoring body must be financially independent and shall have access to adequate financial and other resources to fulfil its monitoring responsibilities, especially for the accreditation of a natural person. This means that it must be in a position to manage its budget and to make autonomous decisions insofar as the expenditure of funds to carry out its functions is concerned. Such independence must be sourced from stability and resources channelled to the operation of the monitoring activities and allocated to meet its liabilities. It is equally important that, as long as financial matters are concerned, the monitoring body is not subject to any external influence, in particular from the code owner and / or from the code members. In the event that the monitoring body obtains any kind of financial support from the latter (e.g. in case of code members paying an association fee), the

[8] See also infra, section 5.

monitoring body must ensure that such source of funding does not adversely affect the independence of the its monitoring duties. It is remarked that the financial independence is not considered to be met in case the rules governing the financial support of the monitoring body do not prevent that a code member, who is under investigation by the same monitoring body, can stop its financial contributions to it, in order to avoid a potential sanction from the monitoring body. The elements be taken into account in the assessment of the financial independence of the monitoring body include:

i.	the size and complexity of the code members (as monitored entities);
ii.	the nature and scope of their activities (as the subject of the code); and
iii.	the risk(s) associated with the processing operation(s).

Financial independence may be demonstrated, inter alia, with:

i.	documented procedures regarding the management of budget and other resources;
ii.	evidence of the means by which the monitoring body obtains the necessary funds to support its monitoring activities;
iii.	explanation as of the source of the financial support obtained to demonstrate that it does not compromise the monitoring body's independence; and / or
iv.	documented evidence of a risk assessment conducted in order to implement internal procedures to avoid any liability claim and to calculate the necessary coverage of potential financial penalties (i.e. insurance and / or financial capital).

4.3 ORGANISATIONAL INDEPENDENCE

The monitoring body shall be organised in a manner which empowers it to act independently from code owners and from the code members whilst performing its tasks and exercising its powers. Organisational independence can be ensured, for example, by means of information barriers between the monitoring body and the code owner and the code members, separate reporting structures, separate operational and personnel management functions, and / or by using different logos or names, as appropriate. The monitoring body remains bound to demonstrate such organisational independence, for example by means of:

i.	payroll system for its personnel which is segregated from the code owner and / or code members;
ii.	the deployment of an analytical accounting systems, meaning an accounting system which would allow to separate the costs and revenues of reserved and competitive activities respectively with

	different responsibility centres; and / or
iii.	logical separation of data between the monitoring body and the code owner, in case of an internal monitoring body. This means that techniques, such as specific keys, should be used to ensure that the code owner cannot access the monitoring body's data.

In addition, the monitoring body shall demonstrate to have appropriate human and technical resources to effectively perform its tasks. The monitoring body shall have an adequate and proportionate number of staff members, which could be demonstrated through:

i.	the procedure to appoint the monitoring body personnel;
ii.	the remuneration of the said personnel, as well as the duration of the personnel's mandate; and
iii.	contract or other formal agreement with the monitoring body.

Furthermore, the monitoring body shall demonstrate that such personnel is conversant with the sector covered by the code concerned and familiar with the risks which may arise from the processing activities addressed by the same code. The monitoring body shall be responsible and shall retain liability for its decisions regarding the monitoring activities. At the same time, it shall be able to safeguard its impartiality in issuing such decisions. When the monitoring body is internal to a code owner, there shall be separate personnel and management, accountability and function from other areas of the code owner, and the latter shall prove that a specific, separated budget is allocated to such body by the code owner. The internal monitoring body shall therefore provide additional information that attest its independence and impartiality, which may include:

i.	documented evidence that the monitoring body has been set up only within a code owner;
ii.	information barriers to shield the monitoring body's independent performance;
iii.	separate personnel; and / or
iv.	distinct management roles.

4.4 ACCOUNTABILITY

By virtue of the principle of accountability, the monitoring body shall demonstrate compliance with data protection legislation and observe the principles relating to processing of personal data enshrined in the Regulation. The monitoring body shall act independently and shall remain liable for its own actions and decision. This independence can be evidenced, for example, by means of formal rules for appointment. In the case of an internal monitoring body, it must be ensured that the powers and the operation of any committees do not interfere with the decision-making process. In addition, an internal monitoring body shall submit evidence to demonstrate that its committees and / or

personnel are free from any commercial, financial and any other form of pressure that might influence the decision-making process. The monitoring body is required to provide with evidence to demonstrate that it the abides by the accountability principle in respect of its decisions and actions, which may include:

i.	formal rules for appointment of its personnel;
ii.	framework for the monitoring body personnel roles;
iii.	reporting lines and decision-making processes;
iv.	complete organigram; and / or
v.	policies to increase awareness amongst its personnel about the governance structures and the procedures in place (including training).

4.5 OTHER FUNCTIONS

The monitoring body may be set-up just for monitoring one or more specific codes and solely carry out such monitoring functions, or it may perform additional duties, such as for example consultation in drafting codes of conduct and promoting data protection co-regulation. In the event that the monitoring body discharges other functions, it must ensure that the requirements set herein are adhered to at all times and that the operations carried out in parallel are not in any manner in conflict with the code monitoring functions. In any case, the independence and conflict of interest requirements shall be upheld. Should the monitoring body perform any function other than the code monitoring, it shall inform the supervisory authority accordingly at application stage.

5. ABSENCE OF CONFLICT OF INTEREST

The monitoring body must have its own personnel and shall be able to exercise its tasks and duties in a manner which does not result in a conflict of interest, and to demonstrate the absence of such conflict of interest. In this regard, the monitoring body must refrain from any action which is incompatible with its tasks and duties. The monitoring body must also ensure that it has the necessary safeguards are in place so that its personnel do not engage in any incompatible occupation, whether gainful or otherwise. The monitoring body must remain free from direct or indirect influence and shall neither seek nor take instructions from any person, organisation or association. To fulfil this, the appointment process of the personnel of the monitoring body shall not be subject to direct or indirect external influence, and their duties shall only be subject to the scrutiny of the same monitoring body, which must act in an independent manner. For example, a conflict of interest subsists in situations where the monitoring body takes instructions directly or indirectly from the code owner, or from the

code members. Conversely, particularly in the case of internal monitoring bodies, the provision of services which are purely administrative in nature, or organisational assistance or support activities by the monitoring body to the code owner and / or to the code members is not likely to pose a conflict of interest. The monitoring body must adopt a pro-active approach identifying any situation which is likely to result in a conflict of interest and it shall implement specific measures and procedures to avoid similar situations or, in case they are encountered, to resolve them. Such internal procedures may include:

i.	regular internal audits of which a section must be dedicated to the absence of conflict of interest;
ii.	remediation plan in the event that a conflict of interest is encountered;
iii.	possibility of opting-out by the auditors, or eviction clauses; and / or
iv.	reflection of the absence of conflict of interest obligation into legally-binding commitments to be undertaken by the personnel of the monitoring body (and by the personnel of the sub-contractor, as the case may be). Such commitments shall introduce the obligation to duly and promptly report to the monitoring body any situation likely to create a conflict of interest.

A monitoring body must be appropriately protected from any sort of sanctions or interference (whether direct or indirect) by the code owner, other relevant bodies (bodies who represent categories of controllers or processors) or code members as a consequence of the fulfilment of its tasks.

6. EXPERTISE

The monitoring body shall have an adequate level of expertise to carry out its role in an effective manner. In this respect, its personnel shall possess an in-depth understanding, knowledge, and experience on the sector of the code subject to monitoring. In order to demonstrate expertise of the staff on specific personal data processing, different interests involved and the risks of the processing activities addressed by the code should also be taken into account. As a minimum, the monitoring personnel shall:

i.	have satisfactory general expertise in data protection law. This must be demonstrated by means of relevant education and / or working experience, as furtherly detailed hereunder: **a. Audit** The monitoring body must demonstrate that its personnel engaged in code monitoring audit functions have experience of at least two full audits and to have received comprehensive and satisfactory training on data protection. Such expertise may be demonstrated by means of audit reports and training syllabus and completion

	certificates; **b. Legal** The monitoring body must demonstrate that its personnel engaged in legal functions have accumulated at least two years of professional legal practice which a focus in data protection (e.g. consultancy, litigation, etc.). Such expertise may be demonstrated with employment contracts and / or engagement forms (if employed), or membership to national bars / law societies (if self-employed); **c. Technical** The technical expertise requirement only applies when this is necessary for the code at stake. If that is the case, the monitoring body must demonstrate that its personnel engaged in technical functions have received detailed training about frameworks for information system security management. Such expertise may be demonstrated with evidence of achievement of a related qualification at level 5 EQF[9] or higher. Technical auditors must have experience of at least two years of professional practice in the field of information system security. Such experience may be demonstrated by means of audit reports.
ii.	have demonstrated expertise on specific personal data processing activities which are the subject matter of the code of conduct. This expertise may be demonstrated with evidence of consulting and / or advisory activities; and / or
iii.	have experience and have received training in the field of auditing, monitoring, or quality assurance activities. These may be demonstrated respectively by means of proof of engagement and by training syllabus / completion certificates.

7. ESTABLISHED PROCEDURES AND STRUCTURES

The monitoring body must demonstrate to have in place established procedures and structures which allow it to perform the following functions:

i.	assess the eligibility of controllers and processors concerned to apply the code;
ii.	monitor compliance with the provisions of the code by code members; and
iii.	carry out reviews of the concerned code's operation.

[9] See Annex II to Council Recommendation of 22 May 2017 on the European Qualifications Framework for lifelong learning and repealing the recommendation of the European Parliament and of the Council of 23 April 2008 on the establishment of the European Qualifications Framework for lifelong learning (2017/C 189/03).

The monitoring body shall remain responsible to ensure that any information entered into its possession whilst carrying out its monitoring functions remains confidential unless it is required to disclose such information, for example by a judicial order, or it is exempt by law. This confidentiality obligation shall be reflected into binding legal commitments to be executed by the personnel of the monitoring body. In any event, the confidentiality obligation shall survive the applicability of the code and the functions of the monitoring body and of its personnel.

7.1 ELIGIBILITY OF CODE MEMBERS

The monitoring body must demonstrate to have comprehensive vetting procedures to adequately assess the eligibility of controllers and processors that apply for code membership. In this regard, the monitoring body shall, at application stage, present:

i.	a complete overview of the requirements to which controllers and processors which intend to apply for membership to a specific code are subject. These requirements must stipulate that the processing of personal data by such controllers and processors fall within the scope of the code concerned, and that they have, at the time of their membership application, the capacity to meet the provisions of the code they are applying for; and
ii.	mechanisms to verify the requirements above. These may include the perusal of applying code members' corporate governance documents, the conduction of audits on the controllers and processors concerned and / or any other tool to effectively ensure that the latter have sufficient capabilities and assets to comply with the rules laid down in the code.

7.2 MONITORING OF COMPLIANCE

The monitoring body must demonstrate that it has a procedure for the investigation, identification and management of code member infringements to the code and additional controls to ensure that appropriate action is taken to remedy such infringements of the code. To achieve this, the monitoring body must be equipped with sufficient powers towards the code members. At the same time, by adhering to the code, the code members must accept to be subject to such powers without reservations. The procedures and structures established by the monitoring body in order to monitor compliance with the code must take into account the risk raised by the specific data processing operations governed by the code, the number of code members, any admissible complaint that has been received by the monitoring body and any other factor which is relevant to the code monitoring. The monitoring body shall have, as a minimum, the power to:

i.	request from a code member any information that the monitoring body may require for the

	performance of its tasks;
ii.	carry out unannounced audits and / or inspections on code members;
iii.	instruct code members to fill-in and submit self-monitoring reports or questionnaires;
iii.	carry out at least an annual inspection in the form of audits on code members;
iv.	act upon the findings of the said audits and inspections and to take corrective action accordingly, as the case may be;
v.	investigate complaints lamenting alleged infringements of the provisions of the code by a code member, as furtherly specified in section 7 below;
vi.	give instructions to code members to bring their practices back into compliance with the provisions of the code;
vii.	suspend or annul the membership of code members and / or to decide that code members which membership has been annulled are no longer entitled to adhere to the code, depending on the severity of the infringement;
viii.	apply the corrective measures as defined in the code; and
ix.	any other investigative and / or corrective power to enable the monitoring body to verify compliance with the code by the code members.

These procedures could lead to the publication of monitoring information including audits, summary reports or periodic reporting of findings, which can be made available to the code owner and / or to the code member, as they case may be.

8. TRANSPARENT COMPLAINTS HANDLING

The code must grant data subjects with the right to file complaints on alleged infringements of provisions of the code with the monitoring body. The monitoring body must have in place effective procedures and structures to handle such complaints in an impartial and transparent manner. When handling complaints, the monitoring body must ensure that:

i.	It is organized in a manner that a dedicated and segregated section of the monitoring body oversees complaints. When this not possible, for example in case the monitoring body is a natural person, a justification shall be brought forward;
ii.	it observes the principle of natural justice[10] and it upholds the right to be heard;
iii.	the complaint-handling process is publicly available. If necessary, the monitoring body should publish guidance to ensure that the process is understandable by data subjects;

[10] General, two-fold legal concept which main components are the notions of *audi alteram partem* and *nemo iudex in causa sua*.

iv.	suitable corrective measures are taken on controllers and processors when an infringement of the code provisions is detected, and that such measures are effective, proportionate and dissuasive and avoid future recurring;
v.	decisions on complaints are published at least in the form of summaries or statistical data; and
vi.	where required and depending on the circumstances of the case, it informs the relevant stakeholders, such as code members, the code owner and the supervisory authorities about the measures taken and of the reason for the decision. In the case of a transnational code, the monitoring body should also inform the identified Lead Supervisory Authority[11] accordingly.

The complaint-handling process must include, as a minimum:

i.	the procedure for the receipt, validation, track, investigation and decision of complaints;
ii.	the high-level requirements for lodging complaints, including the minimum content of a complaint;
iii.	the timing of the complaint-handling process. The process shall dictate that a complainant shall be notified on the progress or outcome of the complaint at the latest within three months from the date of receipt of the complaint;
iv.	the investigative and corrective powers of the monitoring body, which shall include, for instance, the power to suspend or exclude a controller or processor from the code when it acts outside the terms of the code;
v.	the duty for the code members under investigation to provide relevant information to the monitoring body;
vi.	that the decisions taken by the monitoring body on a complaint are subject to revision and the description of the revision procedure;
vii.	that decisions on serious infringements of the code, that for instance determine the exclusion of a code member, are made available to the public;
viii.	the list of sanctions set out in the code of conduct in cases of infringements of the code by a code member. These remedial actions and sanctions could include such measures ranging from training to issuing a warning, report to the Board of the member, a formal notice requiring the implementation of specific actions within a specified deadline, temporary suspension of the member from the code until remedial action is taken to the definitive exclusion of such member from the code. These measures could be publicised by the monitoring body, especially where there are serious infringements of the code.

9. COMMUNICATION WITH THE COMPETENT SUPERVISORY AUTHORITY

[11] As defined in Article 56(1) of the GDPR ("**LSA**").

The monitoring body shall be able to communicate effectively and promptly with the competent supervisory authority and with other supervisory authorities on matters related to the code subject to monitoring. In this respect, the monitoring body shall establish efficient reporting mechanisms and appoint a contact person and a back-up contact person to correspond with the competent supervisory authority, whose details must be made available to the supervisory authorities involved. As a minimum, the monitoring body shall inform the competent supervisory authority without delay about:

i.	decisions where the monitoring body has taken action on infringements by code members, including cases where the monitoring body has ruled the suspension or exclusion of the controller or processor concerned from the code, together with the reasons thereof;
ii.	periodic reports on the status and on the results of the code monitoring activity;
iii.	the outcome of the review of the code or of any relevant audit findings;
iv.	any substantial change that may affect the capacity of the monitoring body to monitor the code, for example, a financial takeover likely to pose a risk to its impartiality; and
v.	any decision about the approval, withdrawal or suspension of the monitoring body taken by its code members without the consultation and approval of the competent supervisory authority.

In case of a transnational code being monitored, the monitoring body shall inform the LSA and the supervisory authorities concerned[12] without undue delay on the elements listed above.

10. CODE REVIEW MECHANISM

It is a requirement that the code sets out appropriate review mechanisms to ensure that the code remains relevant and continues to contribute to the proper application of the Regulation. Review mechanisms shall 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. The code itself must incorporate mechanism to review the code and it remains the responsibility of the code owner to guarantee the continued relevance and validity of the code. The monitoring body and, if appropriate, any other entity referred to in the code of conduct may be granted an active and participative role in the code review process. The monitoring body shall assume a consultative function to the code owner in case an update, review, amendment and / or extension of the monitored code is envisaged or deemed required. To carry out this function in a proper manner, the monitoring body shall have in place:

i.	mechanisms to gather the feedback of code members and other stakeholders with regards to the continued validity and suitability of the provisions of the code;

[12] As defined in Article 4(22) of the GDPR.

ii.	tools to elaborate the results of the consultations indicated above and translate them into proposed amendments and / or extensions to the code, if necessary;
iii.	tools to monitor the introduction of new technological developments which might have an impact on the data processing activities which are governed by the code;
iv.	record-keeping tools to keep track of its monitoring activities, including on actions taken on code members in case of infringements. Referring to these indicators, the monitoring body should be able to define the level of compliance with the code on the basis of measurable and empirical elements, to be communicated to the code owner on a regular basis for further action, as the case may be; and
v.	functional communication channels to correspond with the code owner in a prompt and practical manner, in order to be able to exchange relevant information about the code and about the developments in its application and monitoring.

11.REVOCATION OF A MONITORING BODY

The monitoring body shall commit to fulfil the requirements listed in this document at the time of the application for accreditation and maintain them for the entire duration of its monitoring function. The monitoring body shall therefore demonstrate that it can deliver the code of conduct's monitoring mechanism over a suitable period of time. In case an accredited monitoring body suffers a change which determines the loss of one or more of the requirements for accreditation laid down in this document, and / or may compromise its capacity to carry out the monitoring function, it shall notify to the competent supervisory authority in a timely manner. Such a substantial change may occur, for example, in case key personnel leaves the monitoring body and it is not replaced in a timely manner. In any event, the competent supervisory authority shall retain the power to revoke the accreditation status of the monitoring body, in terms of Article 41(5) of the GDPR. The competent supervisory authority may also decide to revoke the accreditation of the monitoring body in case the latter infringes the provisions of the code, or more in general of data protection law. In such a case, depending on the circumstances, prior to the revocation, the competent supervisory authority should give the monitoring body the opportunity to urgently address the issues encountered and remediate to its infringements by taking the necessary corrective actions. In the case of transnational codes, the competent supervisory authority should consult and seek the views of the concerned Supervisory Authorities and communicate that it intends to revoke the accreditation of the monitoring body to all concerned Supervisory Authorities and to the Board. Taking into account that the revocation of a previously accredited monitoring body may adversely affect the reputation or business interests of the code members and may result in a reduction of trust of data subjects or other stakeholders, as a consequence of such revocation, the code may be suspended or permanently withdrawn. It is

mandatory that the code owner includes relevant provisions in the code to discipline the course of action to be followed in the case of revocation of the accreditation of the monitoring body by the competent supervisory authority.