ICO ACCREDITATION REQUIREMENTS FOR UK GDPR CODE OF CONDUCT MONITORING BODIES

ICO accreditation requirements for a UK GDPR code of conduct monitoring bodies

General Notes:

The UK GDPR introduced a number of data protection requirements for data controllers and processors. It also encourages the development of voluntary compliance activities including codes of conduct in order for data controllers and processors to demonstrate their effective application of the UK GDPR.

Article 41(1) of the UK GDPR states that compliance monitoring of approved codes of conduct may be carried out by an impartial monitoring body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the Information Commissioner.

The UK GDPR sets out a broad framework for the type and structure of a monitoring body, taking into account the code itself and thereby allowing some flexibility. Code owners will put forward proposals for their code monitoring body in accordance with *Article 41(2)* which sets out a number of requirements which the proposed monitoring body needs to meet in order to gain accreditation. Monitoring bodies must:

- Demonstrate independence and expertise in accordance with *Article 41(2)(a).*
- Demonstrate established procedures in accordance with *Article 41(2)(b).*
- Demonstrate established procedures and structures to handle complaints about infringements of the code in accordance with *Article 41(2)(c).*
- Demonstrate that its tasks and duties do not result in a conflict of interest in accordance with *Article 41(2)(d).*

Accreditation Requirements:

Applications for monitoring body accreditation must be submitted in English or Welsh with all supporting documents to the ICO.

The ICO reserves the right to conduct a risk-based review of the monitoring body periodically 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.

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

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

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

1. *Independence*

Explanatory Note:

The requirements below set out what constitutes independence in relation to the subject matter of the code to the satisfaction of the Commissioner in accordance with A41(2)(a) UK GDPR. These rules and procedures will allow the monitoring body to perform its monitoring tasks without influence from members of the code or its code owner.

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

The monitoring body could be an internal or external body as long as evidence can be provided of adequate procedures and rules that allow monitoring of compliance with a code independently and without undue pressure or influence from the code owner or the code members. Internal bodies shall provide evidence to ensure that the independence of their monitoring activities are not compromised.

1.1 Legal and decision-making procedures

Requirements:

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 the code owner itself.

1.1.2 The monitoring body shall demonstrate that it will act independently in its choice and application of its actions and sanctions. This could be evidenced by formal rules for appointment, terms of reference, powers and operation of any committees or personnel that may be involved with an internal monitoring body (such committees or personnel shall be free from any commercial, financial and other pressures that might influence decisions).

1.1.3 The monitoring body shall provide evidence during the application process that its personnel can act independently and without undue pressure or influence in relation to:

a. supervision of resources and finances of the monitoring body;
b. decisions on and performance of compliance monitoring; and
c. safeguarding of impartiality.

Such evidence can include but is not limited to documented recruitment processes, job descriptions, risk registers, risk treatments, meeting minutes and other documented processes as appropriate.

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

1.2 Financial

Requirements:

1.2.1 The monitoring body shall demonstrate that it has the financial stability and resources, for the operation of its monitoring 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 demonstrate to the ICO the means by which it obtains financial support for its monitoring role and explain how this does not compromise its independence.

1.3 Organisational

Requirements:

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

1.3.2 The monitoring body shall demonstrate organisational independence. By way of example, an internal monitoring can demonstrate this with use of different logos or names where appropriate and/or separate reporting or line management structure.

1.3.3 The monitoring body shall demonstrate that it has adequate resources and personnel to effectively perform its tasks, that it is able to act independently from, and is protected from interference or sanctions from code owners and code members as a result of this duty.

1.3.4 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 who will remain ultimately responsible for compliance with its obligations as a monitoring body. This could be demonstrated with evidence that may include:

a. written contacts or agreements to outline for example responsibilities, confidentiality, what type of data will be held and a requirement that the data is kept secure;

b. a clear procedure for subcontracting including the conditions under which this may take place, an approval process, and the monitoring of subcontractors; and

c. sufficient documented procedures to guarantee the independence, expertise and lack of conflicts of interests of the sub-contractors.

1.4 Accountability

Requirements:

1.4.1 The monitoring body shall provide evidence to demonstrate that it is accountable for its decisions and actions, for example, by setting out a framework for its roles and reporting procedures, and its decision-making process to ensure independence. Such evidence could include but is not limited to job descriptions, management reports and policies to increase awareness among the personnel about the governance structures and the procedures in place (eg training).

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.

2. Conflict of interest

Explanatory Note:

In accordance with Article 41(2)(d) UK GDPR the monitoring body must demonstrate to the satisfaction of the Commissioner that its tasks and duties do not result in a conflict of interests. The requirements below aim to ensure that the monitoring body can deliver its monitoring activities in an impartial manner, identifying situations that are likely to create a conflict of interest and taking steps to avoid them.

It will be for the monitoring body to explain the approach to safeguard impartiality and to evidence the mechanisms to remove or mitigate these risks as appropriate. Examples of sources of risks to impartiality of the monitoring body could be based on ownership, governance, management, personnel, shared resources, finances, contracts, outsourcing, training, marketing and payment of sales commission.

Requirements:

2.1 The monitoring body shall have a process to identify, analyse, evaluate, treat, monitor and document on an ongoing basis any risks to impartiality arising from its activities. The monitoring body personnel shall undertake to comply with these requirements and to report any situation likely to create a conflict of interest.

2.2 The monitoring body shall choose or direct and manage its personnel. This could be demonstrated by providing evidence which includes job descriptions, personnel records, recruitment of personnel, resource allocations and line management arrangements.

2.3 The monitoring body shall remain free from external influence and ensure that it does not seek or take instructions from any person, organisation or association, concerning its monitoring functions, that would result in a conflict of interests.

2.4 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:

In accordance with Article 41(2)(a) UK GDPR, the monitoring body must demonstrate its expertise in relation to the subject matter of the code to the satisfaction of the Commissioner. The requirements below aim to ensure that the monitoring body possesses adequate competencies to undertake effective monitoring of a code.

In order for a monitoring body to meet the expertise requirements, it will need to demonstrate that its personnel have the required knowledge and experience in relation to the subject matter of the code, processing activity, data protection legislation and auditing, in order to carry out compliance monitoring in an effective manner. This could be demonstrated to the ICO with evidence that includes personnel job descriptions, specification requirements, qualifications, required or relevant experience, published reports etc.

Requirements:

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

3.2 The monitoring body shall 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 previous experience in auditing, monitoring or quality assurance.

3.3 The monitoring body shall demonstrate that it meets relevant expertise requirements if and where defined in the code of conduct.

4. Established procedures

Explanatory Note:

In accordance with Article 41(2)(b) UK GDPR the monitoring body must demonstrate that it has established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor its compliance with the provisions and to periodically review its operation. The requirements below aim to ensure that the proposals for monitoring are operationally feasible, by specifically outlining the monitoring process and demonstrating how it will deliver the code's monitoring mechanism.

These procedures could lead to the publication of monitoring information including audit or summary reports or periodic outcomes reporting of findings.

The monitoring body shall also apply the appropriate actions as defined in the code of conduct.

Requirements:

4.1 The monitoring body shall demonstrate that it has a procedure to check both the eligibility of controllers and processors to apply for code membership and their ability to comply with code requirements.

4.2 The monitoring body shall demonstrate that it has a procedure to check that potential code members are not the subject of any ICO investigation or regulatory action that might prevent code membership being issued.

4.3 The monitoring body shall demonstrate that it has a procedure to provide periodic compliance monitoring taking into account such things as: the complexity and risks involved, number of code members, geographical scope, complaints received by the monitoring body, and any current or recent ICO investigation/regulatory action.

4.4 The monitoring body shall demonstrate that its audit or review procedures define the requirements to be assessed, the type of assessment to be used and a procedure to document the findings. Review procedures can include such things as: audits, inspections, reporting and the use of self-assessment reports or questionnaires.

4.5 The monitoring body shall demonstrate that it has a procedure for the investigation, identification and management of code member infringements to the code and additional controls to ensure appropriate action is taken to remedy such infringements as set out in the relevant code of conduct.

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 complaints handling

Explanatory Note:

In accordance with Article 41(2)(c) UK GDPR the monitoring body must demonstrate that it has 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.

Transparent and publicly available procedures and structures to handle complaints in relation to both code members and the monitoring body from different sources are an essential element for code monitoring. This process will be sufficiently resourced and managed, and personnel will demonstrate sufficient knowledge and impartiality.

In order to meet these requirements, the monitoring body will need to provide evidence of a documented, independent, and transparent complaints handling process to receive, evaluate, track, record and resolve complaints within a reasonable time frame. We would normally expect the resolution of non-complex complaints to be dealt with within three months.

Requirements:

5.1 Complaints about code members:

5.1.1 The monitoring body shall provide evidence of a clear framework for a publicly available, accessible and easily understood complaints handling and decision-making process.

5.1.2 The monitoring body shall acknowledge receipt of the complaint and provide the complainant with a progress report or the final decision of the investigation within a reasonable time, such as three months.

5.1.3 The monitoring body shall provide evidence of suitable appropriate actions, as defined in the code of conduct, in cases of infringement with the code to stop the infringement and avoid future re-occurrence. Such actions could also include, training, issuing a warning, report to the board of the member, formal notice requiring action, suspension or exclusion from the code.

5.1.4 The monitoring body shall provide evidence of its process for notifying the ICO immediately and without undue delay about the measures taken and justification of any infringements leading to code member suspension or exclusion.

5.1.5 The monitoring body shall maintain a record of all complaints and actions which the ICO can access at any time.

5.1.6 Decisions of the monitoring body shall be made publicly available in line with its complaints handling procedure. This information could include but is not

limited to, general statistical information concerning the number and type of complaints/infringements and the resolutions/appropriate actions issued and shall include information concerning any action leading to suspensions or exclusions of code members.

5.1.7 The monitoring body shall assist in the investigation and resolution of any complaints about code members to the ICO.

5.2 Complaints against the monitoring body:

5.2.1 The monitoring body shall provide evidence of a clear framework for a publicly available, accessible and easily understood complaints handling and decision-making process in relation to complaints made against them.

5.2.2 The monitoring body shall have a documented process to receive, evaluate and make decisions on complaints made about its monitoring responsibilities and activities.

5.2.3 The monitoring body shall assist in the investigation and resolution of any complaints about the monitoring body to the ICO.

5.3 Appeal and complaints about decisions made by the monitoring body:

5.3.1 The monitoring body shall provide evidence of a clear framework for a publicly available, accessible and easily understood complaints handling and decision-making process in relation to complaints made about its decisions.

5.3.2 The monitoring body shall have a documented appeals process which shall be made publicly available, accessible and be easily understood and transparent.

5.3.3 The handling process for appeals shall include at least the following:

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

b. tracking and recording appeals, including actions undertaken to resolve them; and

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

5.3.4 The monitoring body shall acknowledge receipt of the appeal and provide progress reports and the final decision to the relevant party within a reasonable time, such as three months.

6. Communicating with the ICO

Explanatory Note:

In accordance with Article 41(4) the monitoring body shall inform the Commissioner of actions taken that lead to suspension or exclusion of controllers or processors from the code, and the reasons for taking them.

The section below sets out the information the monitoring body will provide to the ICO. This includes information concerning any suspension or exclusion of code members and any substantial changes to its own status.

It is envisaged that suspension or exclusion of code members will only apply in serious circumstances and code members would first have the opportunity to take remedial action as appropriate and agreed with the monitoring body.

The monitoring body is accredited on the basis of fulfilling all requirements at the time of accreditation and continuing to fulfil those requirements in order to effectively perform its function. Any subsequent substantial changes relating to the monitoring body's ability to function independently and effectively, its expertise and any conflict of interests should be immediately communicated to the ICO. This would result in a review of the monitoring body accreditation.

Requirements:

6.1 The monitoring body shall evidence a clear framework to allow for reporting of any suspensions or exclusions of code members to the ICO. This reporting framework shall require as a minimum that the monitoring body will:

a. inform the ICO promptly and in writing of any suspension or exclusion providing valid reasons for the decision;
b. provide information outlining details of the infringement and actions taken; and
c. provide evidence that it has taken action in line with the suspension or exclusion process.

6.2 The monitoring body shall have a documented procedure for lifting the suspension or exclusion of a code member and notifying that code member and the ICO of the outcome of the review or investigation.

6.3 Substantial changes to the monitoring body may include but are not limited to:

a. its legal, financial, commercial, ownership or organisational status and key personnel;
b. resources and any changes to UK legal entity; and
c. any changes to the basis of accreditation.

6.4 The monitoring body shall report any substantial changes to the ICO immediately and without undue delay.

7. Code review mechanisms

Explanatory Note:

In accordance with Article 41(2)(b) UK GDPR the monitoring body must demonstrate that it has established procedures which allow it to periodically review the operation of the code. Monitoring bodies therefore have a key role in contributing to the review of the code and as a result, amendments or extensions may be made to the code by the code owner.

Requirements:

7.1 The monitoring body will contribute to reviews of the code as required by the code owner and shall therefore ensure that it has documented plans and procedures to review the operation of the code to ensure that the code remains relevant to the members and continues to meet the application of the UK GDPR.

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

a. information concerning new members to the code;
b. details of any suspensions and exclusions of code members;
c. confirmation that a review of the code has taken place and the outcome of that review;
d. that there are no substantial changes to the monitoring body; and
e. information concerning data breaches by code members, complaints managed and the type and outcome of monitoring functions that have taken place.

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

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

8. Legal status

Explanatory Note:

The monitoring body may be set up or established in a number of different ways, for example limited companies or trade associations. However, the overarching principle is that whatever form the monitoring body takes, it must demonstrate sufficient financial and other resources to deliver its specific duties and responsibilities. The monitoring body will therefore have to provide evidence to the ICO 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.

A monitoring body is not responsible for code members' UK GDPR compliance.

Requirements:

8.1 The monitoring body shall evidence to the ICO that it has the appropriate standing to meet the requirements of being fully accountable in its role with sufficient financial and other resources; in particular with reference to s149 and s 155 Data Protection Act 2018 and Article 83 of the UK GDPR, being able to take appropriate action in line with Article 41, and that it has access to adequate resource requirements to fulfil its monitoring responsibilities. Such evidence could, depending on the structure of the monitoring body, include (but not be limited to):

a. 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 company or organisation, joint venture, LLP, partnership or other entity; and
b. evidence of appropriate legal transfers of powers and resources to 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.

8.2 The monitoring body shall be a legal entity, or a defined part of a legal entity such that it can be held legally responsible (in accordance with Article 83(4)(c) UK GDPR and S.149 and S.155 DPA 2018) for breaches of its monitoring activities.

8.3 The monitoring body shall be established in the UK.