OFFICE OF
THE DATA PROTECTION OMBUDSMAN

Record no. 572/117/20

29 January 2021

The FI SA accreditation requirements for a GDPR code of conduct monitoring bodies

Introduction

The regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of their personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation (GDPR)) came into effect on 25 May 2018. GDPR 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 GDPR.

According to Article 57(1)(p) GDPR each supervisory authority (SA) shall on its territory draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41. Further, in Article 41(3) is the requirement for the competent SA to submit the draft criteria for accreditation of a monitoring body to the European Data Protection Board (EDPB). Finnish Data Protection Act (1050/2018) determines that the national supervisory authority referred to in GDPR is, in Finland, the Office of the Data Protection Ombudsman (the Finnish supervisory authority (FI SA)).

In this document FI SA drafts above-mentioned requirements for accreditation of the monitoring body. This document should be read alongside articles 40 and 41 GDPR and the EDPB Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 (Guidelines 1/2019). GDPR and Guidelines 1/2019 set out a broad framework for the type and structure of a monitoring body, taking into account the code itself and thereby allowing some flexibility.

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

According to Article 41(2) monitoring bodies must:

- Demonstrate independence and expertise in relation to the subject matter of the code as per Article 41(2)(a).
- Demonstrate established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation as per Article 41(2)(b).
- Demonstrate established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller of processor, and to make those

procedures and structures transparent to data subjects and the public as per Article 41(2)(c).

- Demonstrate to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interest as per Article 41(2)(d).

General notes

Applications for monitoring body accreditation must be submitted in Finnish, Swedish or English with all supporting documents to the FI SA.

The FI SA will review the accreditation of the monitoring body periodically according to risk-based approach to ensure that the body still meets the requirements for accreditation. The review period will be determined in each case in the FI SAs decision concerning the accreditation of the monitoring body. The monitoring body shall communicate with the FI SA which will initiate the review process. Time of communication will be determined in line with the review period. Such a review could also 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 review concludes that the requirements for accreditation are no longer met. The review might result in the revocation of the accreditation of a monitoring body pursuant to Article 41(5) GDPR.

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.

Accreditation Requirements

1 Independence

Explanatory Note

The monitoring body shall be appropriately independent in relation to its impartiality of function from the code members, the profession, industry or sector to which the code applies. It shall also be appropriately independent with regard to any legal and economic links that may exist between the monitoring body and the code owner or code members. Independence of a monitoring body can be understood as a series of formal rules and procedures for the appointment, terms of reference and operation of the monitoring body. These rules and procedures will allow the monitoring body to perform its monitoring tasks without influence from members of the code or its code owner.

The requirements below set out what constitutes independence. The monitoring body requesting accreditation shall demonstrate its independence within the following areas: the monitoring body’s financial resources, appointment of members/staff, decision making procedures and accountability, and organisational structure.

Financial resources

1.1 The monitoring body shall have the financial stability and resources for the operation of its activities and to meet its liabilities. The amount of financial resources

required depend on the risks for data subjects, the sensitivity and complexity of the processing that takes place within the context of the code, the size of the sector concerned, and the expected number and size of the code members.

1.2 The monitoring body shall demonstrate its independence and financial stability in case one or more funding sources are no longer available. The monitoring body shall also demonstrate its financial independence and stability with regard to the risks associated with the activities of the monitoring body itself, for example in case of damages that need to be paid due to the monitoring body's liability. In this respect, the accredited monitoring body shall report to the FI SA when a relevant loss of funding sources occurs or in case of other relevant changes in its funding.

1.3 The monitoring body shall be able to determine allocation of its funds and resources independently and effectively monitor compliance without any form of influence from the code owner or code members. The monitoring body shall demonstrate the amount of budget and resources vested for monitoring the code of conduct in question.

1.4 The monitoring body shall obtain financial support for its monitoring role in a way that does not compromise its independence. The financial support shall not be affected by the actions and decisions of the monitoring body.

1.5 The monitoring body shall deliver to the FI SA contractual clauses or other documentation that demonstrates how it obtains financial support for its monitoring role. The monitoring body would not be considered financially independent for example if the rules governing its financial support allow a code member, who is under investigation by the monitoring body, to stop its financial contributions to it in order to avoid a potential sanction from the monitoring body.

Appointment of members/staff

1.6 The members/staff of the monitoring body shall be appointed via procedure that does not compromise the independence of the body. The members/staff of the body shall be appointed by the monitoring body or some other body appropriately independent of the code.

1.7 The monitoring body shall demonstrate its independence and impartiality and deliver to FI SA general description of the recruitment/appointment processes which cover appropriate mechanisms for identifying and mitigating any risks for its independence.

Decision making procedures and accountability

1.8 The monitoring body shall act independently in performing its tasks and exercising its powers. Decisions and actions of the monitoring body shall be made free from any commercial, financial and other pressures. Any decisions made by the monitoring body related to its functions shall not be subject to approval by any other organisation, including the code owner.

1.9 Members/staff of the monitoring body shall remain free from any external influence and shall be responsible for their decisions regarding the monitoring activities. This could be demonstrated through e.g. terms of the remuneration of the members/staff of the body and/or the duration of the members/staff's mandate.

1.10 Monitoring body shall be accountable for its decisions and actions and shall deliver to the FI SA description of its roles and reporting procedures and its decision-making process to ensure independence. Further, the monitoring body shall deliver to the FI SA its policies to increase awareness (e.g. training) among members/staff about the governance structures and the procedures in place.

Organisational structure

1.11 The monitoring body shall have adequate resources and personnel to effectively and independently perform its tasks. The amount and type of resources required depend on the risks for data subjects, the sensitivity and complexity of the processing that takes places within the context of the code, the size of the sector concerned, and the expected number and size of code members.

1.12 Internal monitoring body can be set up within a code owner. It cannot be set up within a code member.

1.13 The monitoring body shall be protected from any sort of sanctions and interference by code owners or code members as a result of its duty.

1.14 In case of an internal monitoring body, monitoring body's impartiality in relation to the larger entity (for example, the code owner) shall be ensured. An internal monitoring body should have separate members/staff and management. If in an exceptional situation it is not possible for an internal monitoring body to have separate members/personnel and management from the larger entity it belongs to, the monitoring body must demonstrate appropriate safeguards in place to sufficiently mitigate a risk of independence or a conflict of interest. This could be demonstrated for example with documentation concerning information barriers, separate reporting and separate operational and management functions.

1.15 When a monitoring body uses sub-contractors to fulfil some of its tasks, the obligations and requirements for independence, expertise and lack of conflicts of interests are applicable to the sub-contractor in the same way as to the monitoring body. Notwithstanding the sub-contractor's responsibility and obligations, the monitoring body is always the ultimate responsible for the decision-making and for compliance. The use of subcontractors does not remove the responsibilities of the monitoring body. When subcontractors are used, the monitoring body shall ensure effective monitoring of the services provided by the contracting entity.

1.16 The monitoring body cannot outsource its decision-making powers.

1.17 If sub-contractors are used, the monitoring body shall deliver to the FI SA the following information:

- a list of sub-contractors;
- tasks and roles of sub-contractors.

When sub-contractors are used for processes relating to monitoring actions the monitoring body shall also deliver:

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

- documentation of the procedure for subcontracting including an approval process and the monitoring of subcontractors.

2 Conflict of interest

Explanatory Note

The monitoring body shall demonstrate that the exercise of the monitoring body's 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. Conflicts of interest might depend for example on the specificities of the sector(s) to which the code of conduct applies.

In case of an internal monitoring body the requirements relating to the burden proof of absence of conflict of interest will be evaluated in a stricter manner.

Requirements

2.1 The monitoring body shall refrain from any action incompatible with its tasks and duties. The monitoring body shall not provide any services to code members, code owner or other relevant bodies of the sector concerned that would adversely affect its impartiality.

2.2 The monitoring body shall remain free from any external influence and shall neither seek nor take instructions from any person, organisation or association.

2.3 During the recruitment process the monitoring body shall evaluate any risks, such as previous and current tasks, relating to possible impartiality of the person to be appointed/recruited. A conflict of interest could arise for example when personnel conducting audits or making decisions have lately worked for the organisation in question in positions that may compromise their independence or impartiality.

2.4 The staff/member shall be obliged to report any situation likely to create a conflict of interest.

2.5 The monitoring body shall deliver to FI SA a description of the safeguards applied to preventing, detecting and eliminating potential conflicts of interest. This could be demonstrated through e.g. the procedures for recruitment/appointment, terms of the remuneration of the members/staff, the duration of the members/staff's mandate, training programs and internal rules of the monitoring body on accepting gifts or benefits.

3 Expertise

Explanatory Note

The requirements below aim to ensure that the monitoring body possesses adequate competencies and requisite level of expertise to carry out its role in an effective

manner. 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, sector-specific legislation, 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 in-depth understanding of data protection issues and expert knowledge of the specific processing activities which are the subject matter of the code. The monitoring body shall demonstrate compliance with data protection legislation in its own actions. In this respect the monitoring body shall provide information on how it has implemented the principle of accountability in its own actions. This information shall include at least records of processing activities (art. 30 GDPR) of the monitoring body. The FI SA may require delivering additional information and/or documents.

3.2 The monitoring body shall ensure that its personnel carrying out monitoring activities have the required knowledge and experience in relation to the sector, processing activity, data protection legislation and auditing, in order to carry out compliance monitoring in an effective manner.

3.3 The monitoring body shall demonstrate that it meets the expertise requirements above and the relevant expertise requirements as defined in the code of conduct. The monitoring body shall deliver to the FI SA description of expertise that the monitoring body has and documentation that demonstrates how the continuous competence of its members/staff is ensured, such as a training program.

4 Established procedures and structures

Explanatory Note

The monitoring body shall have appropriate governance structures and procedures to assess the eligibility of controllers and processors to apply the code, monitor compliance with the code and to carry out reviews of the code's operation. The requirements below aim to ensure that the proposals for monitoring are operationally feasible and effective.

Requirements

4.1 The monitoring body shall have comprehensive vetting procedure to assess the eligibility of the code members to sign up to and comply with the code. The monitoring body shall deliver to the FI SA the grounds for assessing the eligibility.

4.2 The monitoring body shall have procedures and structures to actively and effectively monitor compliance by code members and review the code's operation. Such procedures and structures shall be designed considering factors such as: the complexity of the processing and risks involved, the size of the sector concerned, expected number and size of code members and complaints received.

4.3 The monitoring body shall have procedures for investigation, identification, documentation and management of code member infringements as well as corrective measures and remedies to them. The procedures need to address the complete

monitoring process, from the preparation of the evaluation to the conclusion of the audit and additional controls to ensure that appropriate actions are taken to remedy infringements and to prevent repeated offences. This shall include a specific control methodology and the documentation and assessment of the findings.

4.4 The monitoring body shall deliver to the FI SA plans for monitoring actions and procedures such as audits, inspections, reporting, use of self-monitoring reports or questionnaires and description of use of the corrective measures determined in the code of conduct in case of infringements of the code by a controller or processor adhering to it. These plans shall include procedures providing for audit plans to be carried out over a definite period and on the basis of predetermined criteria that shall be described in the plans. The monitoring body shall deliver to the FI SA information on how it will manage complaints procedures. It shall outline a procedure to receive, manage and process complaints.

4.5 The monitoring body shall be responsible for the management and confidentiality of all information obtained or created during the monitoring process.

5 Transparent complaints handling

Explanatory Note

The monitoring body shall establish effective procedures and structures to handle complaints in an impartial and transparent manner. The complaint handling process shall be free of charge for the complainant, publicly accessible and sufficiently resourced to manage complaints.

Requirements

5.1 The monitoring body shall have a publicly available, accessible and easily understood complaints handling and decision-making procedure. The description of the procedure shall include at least:

- instructions on how to file a complaint
- contact point for the complainant
- how the complaints are handled and estimated timeframe
- possible outcomes.

5.2 The monitoring body shall deliver the above-mentioned description to the FI SA. The monitoring body shall have suitable corrective measures, defined in the code of conduct, to stop the possible infringement of the code and avoid future re-occurrence. Such corrective measures could also include training, issuing a warning, report to the board of the members, formal notice requiring action, suspension or exclusion from the code. The monitoring body shall deliver description of the corrective measures to the FI SA.

5.3 The data subjects shall be informed about the status and outcome of their individual complaints. The monitoring body has to inform the complainant with progress reports or the outcome of the complaint, within a reasonable time frame. This period

could be extended when necessary, taking into account the size of the organisation under investigation, as well as the size of the investigation.

5.4 The monitoring body shall maintain a record of all complaints it receives, taken actions and outcomes to them. The record shall be accessible to the FI SA on request.

5.5 The monitoring body's decisions, or general information thereof, 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/corrective measures issued and shall include information concerning any sanctions leading to suspensions or exclusions of code members.

5.6 The decisions of the monitoring body shall be published at least when they relate to repeated and/or serious violations, such as the ones that could lead to the suspension or exclusion of the controller or processor concerned from the code.

6 Communication with the FI SA

Explanatory Note

The monitoring body framework needs to include the effective communication with FI SA in respect of the code. This includes information concerning any suspension or exclusion of code members, periodic reports on the code and any substantial changes to its own status. The section below sets out the information the monitoring body shall provide to the FI SA.

Requirements

6.1 The monitoring body shall notify the FI SA immediately and without undue delay about the measures taken and justification of any infringements leading to code member suspension or exclusion.

6.2 The monitoring body shall give to the FI SA annual report with an overview of its activities and decisions. Such a report shall also cover:

- possible audits and inspections
- infringements of the code and actions taken and
- summary of received complaints.

6.3 The monitoring body shall report to the FI SA immediately and without undue delay any substantial changes, such as:

- significant changes to the monitoring body's legal, commercial, ownership or organisational status and key members/staff;
- significant changes to the monitoring body's resources and location(s);
- any changes to the basis of accreditation of the monitoring body;

- significant changes in the number of code members;
- significant loss of funding sources or other significant changes in its funding.

Substantial changes would result in a review of the accreditation.

7 Review mechanisms

Explanatory Note

Monitoring bodies have a key role in contributing to the review of the code in accordance with the review mechanisms outlined in the code to ensure that the code remains relevant to the members and continues to meet the application of the GDPR. As a result of a code review, amendments or extensions to the code may be made by the code owner.

Requirements

7.1 The monitoring body shall contribute to reviews of the code as required by the code or the code owner.

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

- confirmation that a review of the code has taken place;
- possible recommendations for amendments to the code based on the review;
- details of any suspensions and exclusions of code members; and
- information concerning infringements of code members, complaints managed and the type and outcome of monitoring functions that have taken place.

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 or an internal part of the legal entity. Regardless of its legal form, the monitoring body must demonstrate that it has appropriate standing and sufficient financial and other resources to carry out its role and is capable of being fined.

Requirements

8.1 The monitoring body shall be a legal entity, or a defined part of a legal entity such that it is legally responsible for its monitoring activities. The monitoring body shall agree to be responsible for its monitoring role and therefore responsible for a fine under Article 83(4)(c) GDPR and Section 24 Data Protection Act (1050/2018).

8.2 The monitoring body shall have adequate resources for specific duties and responsibilities over a suitable period of time in accordance with the code. The

sufficient financial and other resources shall be accompanied with the necessary procedures to ensure the functioning of the monitoring mechanism over time.

8.3 The monitoring body shall indicate whether it acts as an internal or external monitoring body in relation to the code owner. The monitoring body shall deliver to the FI SA documents related to its legal status. Such documents could depend on the structure of the monitoring body and may include (but not be limited to):

- full company and business name and date and place of incorporation, Memorandum and Articles of Association, details of significant shareholders and directors, registered office and number, ownership and organisation chart, details of interests in or relationship to any other company or organisation (such as joint ventures and partnerships); and

- 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 or undertakings related to monitoring body's legal status.

8.4 The monitoring body shall be established in the EEA.