ACCREDITATION REQUIREMENTS FOR A CODE OF CONDUCT MONITORING BODIES

Version 1.0

Data State inspectorate of the Republic of Latvia

10/2022

TERMS

GDPR - Regulation (EU) 2016/679/EC of the European Parliament and of the Council 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 (General Data Protection Regulation)

SA – data protection supervisory authority

Competent Supervisory Authority – the Data State Inspectorate of the Republic of Latvia

Code of conduct – voluntary accountability tool which set out specific data protection rules for specific categories of controllers and processors.

Accreditation of bodies monitoring compliance with codes of conduct (hereinafter also "**accreditation**") refers to the ascertainment that the proposed monitoring body meets the requirements set out in Article 41 of the GDPR to carry out the effective monitoring of compliance with a code of conduct. This check is undertaken by the supervisory authority where the code is accreditation requirements in relation to monitoring bodies apply individually to each such monitoring body appointed under the code.

Requirements for accreditation of bodies monitoring compliance with codes of conduct (hereinafter also "**accreditation requirements**") refer to the requirements set out in the GDPR Article 41 to carry out the monitoring of compliance with a code of conduct and further specified in this document.

Body monitoring compliance with code of conduct (hereinafter "**monitoring body**") refers to a body/committee or a number of bodies/committees (internal or external to the code owners) who carry out the monitoring**.**

Monitoring refers to procedures (of carrying out the monitoring function) applied by the monitoring body (internal or external to the code owners) to ascertain and assure that the code is complied with according to the Article 41 of the GDPR.

Monitored entity refers to an entity that adhered to the code and selected a monitoring body.

Code Owner refers to association or other body who draw up and submit their code and has an appropriate legal status as required by the code and in line with national law.

National code refers to a code which covers processing activities contained in one Member State.

Transnational code refers to a code which covers processing activities in more than one Member State.

INTRODUCTION

The GDPR determines the responsibility of controller and processor for personal data processing and encourages the development of voluntary compliance activities including codes of conduct for data controller and processor to demonstrate an effective application of the GDPR. The main purpose of codes of conduct is to operate as a rulebook for controllers and processors for data processing activities. Codes must be drawn up by taking into account the specific characteristics of processing carried out in certain sectors and specific needs of controllers and processors and formulating the best practices and practical solutions on personal data protection.

In accordance with Article 57(1)(p) of the GDPR each SA (including Competent Supervisory Authority) shall on its territory draft and publish the criteria for accreditation of a body for monitoring codes of conduct (i.e. this document) pursuant to Article 41 of the GDPR, by which the Monitoring body has:

- demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the Competent Supervisory Authority;

- 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;

- 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; and

- demonstrated to the satisfaction of the Competent Supervisory Authority that its tasks and duties do not result in a conflict of interests.

The monitoring body shall be accredited by the Competent Supervisory Authority in accordance with the GDPR, Personal Data Processing Law[1] (Latvian national law) and regulation of the Cabinet of Ministers No.488 "Licensing rules for the Code of Conduct Authority[2]" (Latvian national law).

Regulation of the Cabinet of Ministers No.488 – "Licensing rules for the Code of Conduct Authority[3]" specifies requirements for the receipt of accreditation license, as well as the procedures for issuing, suspending, and withdrawing the accreditation license, the amount of the State fee and the procedures for transferring the payment.

The period of validity of an accreditation of a monitoring body is 5 years. The accreditation of a monitoring body applies only for a specific code, however, a monitoring body may be accredited for more than one particular code, provided it satisfies the requirements for accreditation each one separately. This document contains the accreditation requirements for monitoring body in accordance with Article 41 (1) of the GDPR and has been prepared and should be read alongside with articles 40 and 41 of the GDPR and the Guidelines of the European Data Protection Board 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679[4].

[1] Personal Data Processing Law, https://likumi.lv/ta/en/en/id/300099-personal-data-processing-law
[2] Regulation of the Cabinet of Ministers No. 488 "Licensing rules for the Code of Conduct Authority"
[3] Regulation of the Cabinet of Ministers No. 488 "Licensing rules for the Code of Conduct Authority"
[4] Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 | European Data Protection Board (europa.eu) Version 2.0, 4 June 2019.

The monitoring of approved codes of conduct will not apply to processing carried out by public authorities or bodies in accordance with section 15 of the Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 | European Data Protection Board (europa.eu) Version 2.0, 4 June 2019. This exemption does not in any way dilute the requirement for the implementation of effective mechanisms to monitor a code.

In the context of monitoring codes of conduct intended to international transfers, the EDPB "Guidelines 04/2021 on Codes of Conduct as tools for transfers"[5] could be used.

1. GENERAL REQUIREMENTS AND APPLICATION

1.1. Applicants shall fulfil all the accreditation requirements set out in this document to become accredited by Competent Supervisory Authority.

1.2. Accreditation of a monitoring body is only possible in a particular industry with particular needs of one or more specific codes of conduct pursuant to Article 41 (1) GDPR, Personal Data Processing Law[6] (Latvian national law) and regulation of the Cabinet of Ministers No. 488 "Licensing rules for the Code of Conduct Authority[7]" (Latvian national law). Each code is evaluated separately, taking into account the industry and its specifics.

1.3. National applications for monitoring body accreditation (hereinafter also - application) shall be submitted in writing to Competent Supervisory Authority[8]. Competent Supervisory Authority accepts only applications in Latvian language, even when submitting the transnational application, a translation into Latvian must be attached in accordance with Latvian Official Language Law. The application shall contain proof of fulfilment of the requirements (submission of relevant documents, certificates etc.) as set out in these requirements.

1.4. The assessment of the application shall consider the specifics of relevant sector.

1.5. In addition to the documents specified in the Regulation of the Cabinet of Ministers No 488[9] the application shall include following information:

a) information identifying the applicant which in either case has the status of a legal entity in the Republic of Latvia or another member state of the European Union or the European Economic Area (full name of legal person, legal status, address, telephone number, contact email address);
b) relevant contact information (if any) to be used for communication between the applicant and Competent Supervisory Authority;
c) specification of the code of conduct for which the accreditation is being applied, including subject-matter of the code of conduct;
d) the scope of the code of conduct (national or transnational);

[5] Guidelines 04/2021 on Codes of Conduct as tools for transfers | European Data Protection Board (europa.eu)
[6] Personal Data Processing Law, https://likumi.lv/ta/en/en/id/300099-personal-data-processing-law
[7] Regulation of the Cabinet of Ministers – "Licensing rules for the Code of Conduct Authority" No.488
[8] Submissions are accepted signed by hand (sent by mail or placed in the Inspector's mailbox) or sent signed with a secure electronic signature to pasts@dvi.gov.lv or the official electronic address (via www.latvija.lv).
[9] Article 3 of Regulation of the Cabinet of Ministers – "Licensing rules for the Code of Conduct Authority" No.488 https://likumi.lv/ta/id/334670-ricibas-kodeksa-parraudzibas-institucijas-licencesanas-noteikumi

e) supporting documents and any information or documents attached to the application providing evidence that the accreditation requirements set out below are fulfilled;
f) results of the code of conduct monitoring audit;
g) the application should contain the written confirmation that, at the time of application and during the activity of the monitoring body all requirements in point 3.2. are met.

1.6. Competent Supervisory Authority reserves the right to conduct reviews of the monitoring body at any time to ensure that the body still meets the requirements.

2. INDEPENDENCE AND ACCOUNTABILITY OF THE MONITORING BODY

2.1. Legal and decision-making procedures.

2.1.1. The monitoring body can act as an internal or external monitoring body vis-à-vis the code owner with the choice of a particular approach at the discretion of the code owner.

2.1.2. The monitoring body shall:

a) comprise of either a for-profit or non-for-profit legal person, which must be registered and operating in the EEA[10];

b) be appropriately independent in relation to its impartiality of function from the code members and the profession, industry or sector to which the code applies, particularly regarding any legal and economic link that may exist between the monitoring body and the code owner or the code members;

c) implement an appropriate decision-making procedure to ensure its full autonomy and independence;

d) act independently in its choice and application of its actions and sanctions against a controller or processor adhering to the code;

e) provide evidence during the application process that the body and its personnel can act independently and without undue influence;

f) not provide any services to code members or the code owner that can adversely affect its independence in performing its tasks and exercising its power.

The independence of the monitoring body in relation to legal and decision-making procedures may be demonstrated by formal rules for appointment to members/staff, terms of reference and job descriptions, documented recruitment processes for its personnel, declaration from persons of the monitoring body authorized to make decisions that shows there are no common interests with the entities to be monitored, description of the owner or owners of the code, information on the duration or expiration of the monitoring body. Evaluation on and treatment of risks regarding independence and/or conflict of interest and/or impartiality, including which internal procedures are implemented to avoid preclusive circumstances and mitigate residual risks. Monitoring body will need to identify risks to its independence, possible conflicts of interests and impartiality on an ongoing basis, such as its activities or from its relationships. If a risk is identified, the monitoring body should demonstrate how it removes or minimizes such risk and uses an appropriate mechanism for safeguarding independence and/or

[10] European Economic Area, as established in the Agreement on the European Economic Area.

impartiality or to avoid conflict of interest.

2.2. Financial resources.

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

2.2.2. The monitoring body shall be able to manage its budget and resources independently without any form of influence from the code owner and the code members.

2.2.3. The means by which the monitoring body obtains financial support (for example, a fee paid by the members of the code of conduct) shall not adversely affect its independence in relation to the task of monitoring compliance with the Code.

2.2.4. The monitoring body shall be able to demonstrate that it has the financial stability and resources to carry out its monitoring activities effectively and consistently. For instance, the monitoring body would not be considered financially independent if the rules governing its financial support allow a code member, who is under investigation by the monitoring body, to stop its financial contributions to it, in order to avoid a potential sanction from the monitoring body.

2.2.5. The monitoring body shall be able to demonstrate (with necessary procedures) sufficient financial resources to ensure its long-term financial stability and its independence of the performance of its tasks.

2.2.6. The monitoring body during the application shall demonstrate to Competent Supervisory Authority the process of means by which it obtains financial support and explain how this does not compromise its independence.

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

2.2.8. In case of an internal monitoring body it has a specific separated budget that the monitoring body is able to manage independently.

The independence of monitoring body in relation to financial resources may be demonstrated by documentation of sources of income, previous, current or projected income and expenses, documents of specific rules in case when one or more funding sources are no longer available (e.g. in case of loss, exclusion of one or more members when monitoring body is financed through code member's contributions).

2.3. Organisational resources and structure.

2.3.1. The monitoring body shall:

a) be organised in a way that enables it to act independently from code owners;

Including it has payroll system for its personnel which is segregated from the code owner and/or code members.

b) have enough human and technical resources necessary for the effective performance of its tasks,

c) be composed of an adequate and proportionate number of personnel (in-house personnel or external personnel),

d) be accountable and retain authority for its decisions regarding the monitoring

activities,

Including internal binding procedures to ensure enforceability and supervision of compliance by the code members with the decisions taken by the monitoring body.

e) be able to act free from instructions and shall be protected from any sort of sanctions or direct or indirect influence.
f) In addition, with 2.3.1.a-e, in cases where an internal monitoring body is proposed, there should be separate staff and management, accountability system and administrative function from other areas of the organisation.

This may be achieved in a number of ways, for example, the use of effective organisational and information barriers and separate reporting management structures for the association and monitoring body.

Organisational aspects could be demonstrated through the procedure to appoint the monitoring body personnel, the remuneration of the said personnel, the duration of the personnel's mandate, through contract or other formal agreement with the monitoring body.

2.3.2. The monitoring body shall demonstrate its organisational independence to Competent Supervisory Authority during the application process.

Including it may be demonstrated by procedures for identification of risks to its organisational independence and how it will remove and minimize such risks and use an appropriate mechanism for safeguarding impartiality.

2.3.3. If the monitoring body uses **sub-contractors** to fulfil some of its tasks, the obligations and requirements for independence, expertise, and absence of conflicts of interests are applicable to the sub-contractor in the same way as to the monitoring body. The use of subcontractors does not remove the responsibilities of the monitoring body and monitoring body shall ensure effective monitoring of the services of sub-contractors. In any case, the monitoring body remains responsible for monitoring compliance with the code to Competent Supervisory Authority.

2.3.4. When engaging a sub-contractor, the monitoring body shall make certain that:

a) the monitoring body remains liable towards all stakeholders in lieu of the sub-contractor;

b) the sub-contractor conforms to the same requirements which apply to the monitoring body;

c) 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, confidentiality, what type of data will be held and a requirement that the data is kept secure;

d) the monitoring body ensures effective monitoring of the services provided by subcontractors;

e) procedures that establish the actions to be taken in the event of a conflict of interest between the monitoring body and the sub-contractors, are documented;

f) specific requirements relating to the termination of contracts and agreements to ensure that all subcontractors will meet data protection obligations of the GDPR.

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

2.3.6. If sub-contractors are used, the monitoring body shall provide Competent Supervisory Authority with the following information:

a) a list of sub-contractors;

b) tasks and roles of sub-contractors.

2.4. Accountability.

2.4.1. The monitoring body shall be able to demonstrate that its decisions and actions are independent.

2.4.2. decisions made by the monitoring body, as part of its monitoring functions, shall not be subject to approval by any other body, association or organisation including the code owner, the members of the code or the profession, industry, or sector the code applies to.

2.4.3. The monitoring body shall provide evidence to Competent Supervisory Authority on its impartiality in relation to accountability during the application process.

It may be demonstrated by:

reporting and working procedures;

formal rules for appointment and tasks of personnel;

internal policies, e.g. adopting staff training policies;

allocation of appropriate roles and structures in organisation;

description of the decision-making process by the monitoring body.

3. REQUIREMENTS RELATING TO THE ABSENCE OF CONFLICT OF INTEREST.

3.1. The monitoring (internal or external) body shall:

a) refrain from any action incompatible with its tasks and duties and shall not provide any services to code members that would adversely affect its impartiality;

b) be protected from any sort of sanctions or influence (whether direct or indirect) by the code owner, other relevant bodies, or members of the code as a consequence of the fulfilment of its tasks;

c) remain free from any external influence (whether direct or indirect,) and shall neither seek nor take instructions from any person, organisation, or association;

d) identify situations that are likely to create a conflict of interest (due to its personnel, its organisation, its procedures, etc.) and provide internal procedures to deal with it, for example, procedure on accepting gifts or benefits;

e) has its own personnel that are chosen by the monitoring body or some other body independent of the code owner. The personnel shall be subject to the exclusive direction of the monitoring body and that other body independent of the code only;

f) carry out regular internal audits;

g) evaluate any risks during the recruitment process, such as previous and current tasks, relating to possible impartiality of the person to be appointed/recruited;

h) be obliged to report to Competent Supervisory Authority about any situation

which is likely to create a conflict of interest when it comes to its personnel and work shall be reallocated;

i) performs awareness training programs for personnel.

An example of a conflict-of-interest situation would be the case where personnel conducting audits or making decisions on behalf of a monitoring body had previously worked for the code owner, or for any of the organisations adhering to the code.

3.2. The monitoring body shall ensure that at the time of application and during the activity of the monitoring body:

a) there exist no relationships that may have an impact between the monitoring body and any code member/s;

b) no personnel of the monitoring body is in a relationship that may have an impact with the code owner or members;

c) if any of the documents or information is already at the disposal of Competent Supervisory Authority the applicant monitoring body may submit a confirmation that there are no changes in the document or information previously submitted to Competent Supervisory Authority.

The monitoring body's description of the safeguards applied to prevent, detect, and eliminate potential conflicts of interest and any incompatible occupation may be demonstrated by the procedures for recruitment/appointment, job descriptions, the terms of remuneration of the personnel, including management personnel, statutory body or stakeholders if applicable, the duration of the personnel's mandate, training programs, the internal rules of the monitoring body on accepting gifts or benefits, internal audits, templates of forms for avoiding of conflict of interest of personnel and enabling the personnel (also subcontractors) to report a conflict of interest.

4. REQUIREMENTS RELATING EXPERTISE

4.1. The monitoring body shall demonstrate that its personnel have requisite level expertise to carry out its monitoring functions accurately and effectively regarding the specific code of conduct.

4.2. The monitoring body shall demonstrate that the personnel taking decisions regarding the monitoring functions have, whether individually or as a whole:

a) in-depth understanding and expert knowledge in relation to data protection law, data protection issues, legal and IT/technical terms and specific legal and practical issues that might be relevant in regard to each specific case;

b) in-depth understanding and expert knowledge in the specific sector and the processing activities which are the subject matter of the code of conduct;

c) in-depth understanding and expert knowledge in carrying out supervisory and control functions (e.g. in the auditing, monitoring or quality assurance activities or in equivalent field);

d) previous experience of acting in a monitoring capacity.

4.3. The monitoring body shall demonstrate that the level of knowledge and experience in the above-mentioned fields is appropriate to effectively carry out its monitoring functions with regard to the code of conduct accreditation is being applied for, by taking into account:

a) the specific sector(s) where the code applies to;

b) the categories of processed data and the complexity of the processing;

c) the individual interests involved;

d) the type and (expected) number of code members;

e) the risks to data subjects.

4.4. The monitoring body shall demonstrate that:

4.4.1. it meets the specific expertise requirements set out in the code of conduct and other factors such as the size of the sector concerned, the different interests involved and the risks of these processing activities.

4.4.2. there are clear role descriptions regarding knowledge and experience requirements both for staff performing the monitoring function and the personnel that is making the decisions.

4.5. The monitoring body shall ensure that the expertise of its personnel is the subject of regular training activities by having regard to the developments in the sector covered by the Code of Conduct in the applicable legislation and/or technological advances. Technical requirements of the personnel will depend on whether it is necessary for the code at stake.

4.6. The personnel with a **legal profile** shall hold:

a) Bachelor's degree qualification in the legal field or equivalent degree and at least three years of a relevant level of experience in accordance with the code itself, or

b) Master's degree qualification or equivalent degree in the legal field and a relevant level of experience in accordance with the code itself of at least one year.

4.7. The personnel with a **technical profile** shall hold:

a) Bachelor`s or Master`s degree qualification in the field of technical/computer sciences, information systems or cybersecurity or equivalent degree and at least three years of a relevant level of experience in accordance with the code itself, and

b) have undergone certificated training on relevant standards for information system security management (regulations, standards, methods, best practices, risk management, etc.).

4.8. The personnel with **an audit profile** shall hold:

a) Bachelor`s or Master`s degree qualification in the field of audit/risk management and a relevant level of experience in accordance with the code itself of at least one year.

4.9. **The monitoring body's evidence of the expertise may be demonstrated by:**

a) description of the competencies, qualifications, and previous experience of the personnel in the monitoring body;

b) documentation of training of the personnel for carrying out the monitoring of compliance with the code and data protection certificates;

c) providing university degrees, postgraduate or master's degree diplomas.

5. MONITORING BODY`S ESTABLISHED PROCEDURES AND STRUCTURES

5.1. The monitoring body shall be able to demonstrate that it has introduced appropriate governance procedures and structures in place that actively, regularly, and effectively monitors compliance with the code by the code members.

5.2. The monitoring body shall also be able to demonstrate that it has appropriate governance structures and procedures which allow it to adequately:

a) assess for eligibility of controllers and processors to apply the code;

b) to monitor compliance with its provisions; and

c) to carry out reviews of the code's operation.

5.3. The monitoring body shall introduce:

a) comprehensive vetting procedures to assess the eligibility of the controllers and processors to sign up to and comply with the code prior to joining the code. The monitoring body shall inform Competent Supervisory Authority about procedures of assessing the eligibility;

b) regular procedures and structures to actively and effectively monitor compliance by code members and review the code's operation, for example random or unannounced audits, annual inspections, regular reporting and the use of questionnaires. Such procedures 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 or specific incidents and the number of members of the code. It could be demonstrated by the publication of audit reports as well as to the findings of periodic reporting from controllers and processors within the scope of the code;

c) 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.

d) adequate resources and staffing to carry out its tasks in an appropriate manner. Resources should be proportionate to the expected number and size of code members, as well as the complexity or degree of risk of the relevant data processing.

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

5.5. The monitoring body shall archive documentation relating to the monitoring of code of conduct under the Latvian national law requirements on archives.

The monitoring body's procedures and structures during the application process may be demonstrated by:

plans for controls (initial, ad-hoc, and recurring) to be carried out over a definite period based on predetermined criteria including type and number of code members, geographical scope, complaints received, established infringements, etc.;

a specific control methodology regarding the type of control to be deployed (self-assessment, audits, inspections with or without prior notice, both onsite and remote, questionnaires, regular reporting, etc.), the criteria to be controlled and the

arrangements to document and manage the findings;

integrity and traceability of evidence when collecting necessary information;

assessment of the findings to detect, investigate and manage, in compliance with the principles of participation, impartiality and equality, any violations of the code of conduct by the members and to adopt appropriate corrective measures, including sanctions, within a reasonable period in order to remedy those infringements and prevent their re-occurrence in accordance with the provisions made in the code of conduct for any breach of its rules;

documented process which ensures that the code members shall fully cooperate with monitoring body to enable carrying out effective controls.

6. TRANSPARENT COMPLAINTS HANDLING

6.1. The monitoring body will need to establish effective procedures and structures which can deal with complaints handling in an impartial and transparent manner. Monitoring body should have:

a) a publicly accessible complaints handling process which is sufficiently resourced to manage complaints and to ensure that decisions of the body are made publicly available;
b) an easily understandable complaint handling and decision-making procedure;
c) in the situation when the controller or processor from the code acts outside the terms of the code - an immediate suitable measures, defined in the code of conduct, to stop the infringement of the code and avoid future recurrence, such as training, issuing a warning, reporting to the Board of the members, 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, or exclusion from the code. These measures could be publicised by the monitoring body, especially where there are serious infringements of the code;
d) the description of the procedure shall include instructions on how to file a complaint, contact point for the complainant, instructions on how the complaints are handled and estimated time frame, possible outcomes. In its procedures, the monitoring body shall include a right of the complainant and the code member to be heard;
e) shall maintain a record of all complaints it receives, taken actions and outcomes to them. The record shall be accessible to Competent Supervisory Authority on request;
f) shall demonstrate its complaint handling procedures and structures during the application process.

6.2. The data subjects shall be informed about the status and outcome of their individual complaints.

6.3. The Monitory body`s decisions or general information shall be publicly available according to complaints handling procedure. It may include 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.

6.4. The decisions of the monitoring body after anonymization of any personal data concerning data subjects shall be published if it relates to violations, such as the ones that could lead to the suspension or exclusion of the controller or processor concerned from the code. Specification of the controller and processor – addressee of those measures shall be also publicly available unless there is another reason obliging to anonymize it.

7. COMMUNICATION WITH COMPETENT SUPERVISORY AUTHORITY

7.1. The monitoring body shall:

a) set out clear reporting mechanisms, including but not only, on any case of a conflict of interest for reporting to Competent Supervisory Authority without undue delay and those situations referred to in point 7.2.;

b) be able to provide all relevant information of any of its actions upon the request of Competent Supervisory Authority;

c) apply and implement updates, amendments, and/or extensions to the Code, as decided by the code owner.

7.2. The monitoring body shall inform Competent Supervisory Authority about:

a) decisions where the monitoring body has acted on infringements by code members, outlining details of the infringement;

b) provide information and evidence of the actions taken;

c) periodic reports on the status and on the results of the code monitoring activity;

d) the outcome of the review of the code or of any relevant audit findings;

e) any decision about the approval, withdrawal or suspension of the monitoring body taken by its code members without the consultation and approval of competent supervisory authority;

f) any substantial change that may affect the capacity of the monitoring body to monitor the code. Substantial changes include but are not limited to any changes that impact the ability of the monitoring body to perform its tasks in an independent, impartial, and efficient manner. It may include changes to the monitoring body's legal, commercial, ownership or organisational status and key personnel, changes to resources and locations, any changes to the basis of accreditation, any other information, which is likely to call into question its independence, expertise, and the absence of any conflict of interests or to adversely affect its full operation;

g) provide the annual report prepared by the monitoring body that includes reviews and/or changes made to the code;

h) provide effective communication of any actions carried out by a monitoring body to the Competent Supervisory Authority in respect of the code.

This could include decisions concerning the actions taken in cases of infringement of the code by a code member, providing periodic reports on the code, or providing review or audit findings of the code.

8. CODE REVIEW MECHANISM

8.1. The monitoring body shall set out appropriate review mechanisms to ensure that the code remains relevant and continues to contribute to the proper application of the GDPR,

including:

a) contribute to reviews, including the need for amending or extending;

b) 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, information concerning infringements of code members, complaints managed and the type and outcome of monitoring functions that have taken place.

8.2. The monitoring body's review may be demonstrated during the application process by:

a) review mechanism and procedures to adjust the code of conduct which envisage the developments in the application and interpretation of the law;

b) review mechanism and procedures to adjust the code of conduct for cases when new technological developments may have impact on the code of conduct.

9. REQUIREMENTS RELATING LEGAL STATUS

9.1. The monitoring body shall:

a) have the appropriate standing to carry out its role under Article 41(4) of the GDPR and is capable of being fined as per article 83 (4) of the GDPR;

b) have a status of legal entity in the Republic of Latvia or in EEA;

c) have appropriate resources for specific duties and responsibilities over a suitable period 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.

9.2. The monitoring body's legal status may be demonstrated during the application process by:

a) memorandum and articles of association;

b) details of ownership and organisation chart;

c) details of interests in or relationship to any other company or organization.