Deliberation 2020-050 of April 30, 2020National Commission for Computing and LibertiesLegal status: In force Date of publication on Légifrance: Tuesday July 28, 2020NOR: CNIL2019163XDeliberation No. 2020-050 of April 30, 2020 adopting a reference system relating approval of bodies responsible for monitoring compliance with codes of conductThe National Commission for Data Processing and Liberties,

Having regard to Convention No. 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data;

Having regard to 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 personal data and on the free movement of such data, and repealing Directive 95/46/EC, in particular its articles 41 and 57.1.p);

Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms;

Having regard to decree n° 2019-536 of May 29, 2019 as amended, taken for the application of law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms;

Having regard to the guidelines on codes of conduct and the supervisory bodies for these codes within the meaning of Regulation (EU) 2016/679 adopted on June 4, 2019 by the European Data Protection Board; After having heard Mrs Anne DEBET, Commissioner , in her report, and Ms. Nacima BELKACEM, Government Commissioner, in her observations, Makes the following observations: Article 41 of the General Data Protection Regulation (GDPR) provides that monitoring compliance with a code of conduct can be carried out by an organization that has the appropriate level of expertise with regard to the subject of the code. These bodies must be approved for this purpose by the competent control authority.

Article 57.1.p) of the GDPR provides that each supervisory authority draws up and publishes the requirements relating to the authorization of bodies responsible for monitoring codes of conduct pursuant to Article 41.

Article 41.3 of the GDPR indicates that the draft authorizations drawn up by each supervisory authority at national level are subject to the consistency control mechanism and must be communicated to the European Data Protection Board (EDPB).

On 3 October 2019, a draft authorization was adopted by the Commission and submitted to the EDPS on 18 October 2019.

The EDPS adopted a favorable opinion on this draft on 28 January 2020, which was notified to the Commission on 4 February 2020.

This deliberation sets the criteria for the approval of bodies responsible for monitoring compliance with codes of conduct, as

referred to in Article 41 of Regulation (EU) 2016/679.

Decided :

The adoption of the accreditation reference system for bodies responsible for monitoring codes of conduct, as appended to this deliberation.

The duration of the approval will initially be set at five years, without prejudice to the exercise at any time of the powers of the CNIL with regard to the obligations of the inspection body.

The procedure for initial application and renewal of an authorization is governed by the internal regulations of the CNIL. The renewal entails a re-examination of the eligibility of the inspection body, which may give rise to a favorable decision or a refusal.

This decision will be published in the Official Journal of the French Republic.ANNEXREFERENCE FOR APPROVAL OF BODIES RESPONSIBLE FOR MONITORING COMPLIANCE WITH CODES OF CONDUCT General comments:

Article 40.4 of the GDPR provides that codes of conduct include the mechanisms allowing the body referred to in Article 41 of the Regulation to monitor compliance with the code. These bodies can be internal or external (as an ad hoc committee). The following requirements apply to all inspection bodies, whether internal or external.

The supervisory authority mentioned in the guidelines below designates the CNIL.

Requirements

1. General requirements

Explicative note :

These requirements aim to establish a general framework for the activities of the inspection body. They also relate to the guarantees that it must provide in order to demonstrate the proper management of its activities as well as its financial and material independence.

1.1 The supervisory body implements a process to ensure that all the processing it carries out as part of its missions complies with the GDPR.

1.2 The monitoring body must demonstrate that all of its human, financial and material resources are commensurate with the scope of the code of conduct. These resources are adapted to the number and size of the members as well as to the complexity or level of risk of the processing implemented by the members.

1.3 The obligations and the essential elements of the function of the inspection body are provided for in the code of conduct.

1.4 The control body ensures that the documents related to the exercise of its missions (documentation provided, audit plan, audit evidence, audit report, etc.) are kept in such a way as to preserve their confidentiality or are permanently and securely destroyed if they are no longer useful after the control mission (subject to other legal obligations or legitimate reasons).

1.5 The inspection body ensures that, in carrying out its missions, the security measures provided for by the member are respected by the inspection body.

These security measures must not prevent the inspection body from carrying out its missions.

2. Requirements relating to the independence of the monitoring body

Explicative note :

The independence of a control body is guaranteed by the establishment of formal rules and procedures governing its appointment, mandate and operation. As part of its application for approval from the supervisory authority, the supervisory body must demonstrate its functional, material and decision-making independence. Compliance with each requirement will be assessed against the evidence provided.

The requirements and examples listed below apply to the monitoring body, whether internal or external.

2.1 The inspection body must demonstrate the principle of its independence, in particular vis-à-vis the bearer of the code, members and professionals in the sector concerned.

2.2 The inspection body must demonstrate its functional independence vis-à-vis the code holder and code adherents in the performance of its tasks and the exercise of its powers.

The inspection body must have the human and technical resources necessary for the effective performance of its tasks. The supervisory body must establish that it is thus able to fully exercise its supervisory functions, taking into account the sector concerned and the risks associated with the processing activities covered by the code of conduct.

2.3 The monitoring body must demonstrate its financial independence by establishing that it has sufficient funding and financial viability to carry out its tasks.

The inspection body must demonstrate that the rules relating to its funding prevent any risk of its independence being impaired or the performance of its tasks being impaired, in particular by a member.

2.4 The monitoring body must demonstrate its independence during the decision-making process, including with regard to the

selection of its personnel responsible for monitoring tasks.

2.5 The inspection body must establish that it is the sole decision maker in the context of its inspection activities.

Without prejudice to the missions and powers of the supervisory authority, the decisions taken by the supervisory body in relation to its functions are not subject to the approval of another body, including the code holder.

3. Requirements relating to the absence of conflict of interest

Explicative note :

The absence of conflicts of interest is guaranteed by the implementation of measures and procedures aimed at preventing such situations.

3.1 The inspection body must remain free from any external influence, direct or indirect.

He must neither seek nor accept instructions from persons, organizations or associations.

3.2 The inspection body must be able to identify any situation likely to create a conflict of interest (due to its personnel, organization, procedures, subcontractors, etc.)

3.3 The organization must put in place procedures and measures to avoid conflicts of interest, so that it refrains from any action incompatible with its tasks and functions.

The regulatory body must provide a procedure for dealing with any situation likely to create a conflict of interest.

3.4 The inspection body must have its own personnel chosen by it or by a service provider independent of the code.

4. Requirements relating to the expertise of the inspection body

Explicative note :

Each application for approval is assessed in concrete terms, also taking into account the specific expertise requirements defined by the code concerned.

The expertise requirements are defined taking into account various factors such as the sector of activity concerned by the code of conduct, the size of this sector, the number of members of the code, the risks linked to the processing activities and the various interests at stake.

4.1 Requirements for senior decision-making personnel

4.1.1 The inspection body must demonstrate that it has the necessary skills to carry out the inspection activities of the code concerned.

4.1.2 The oversight body should demonstrate that decision-making staff have in-depth knowledge and experience of data protection issues and concerns and the specific area of the code of conduct, as well as relates to the exercise of control missions.

These skills are not necessarily combined in one and the same person.

4.2 Requirements for personnel performing control activities

4.2.1 Staff should be trained in auditing methods (auditing principles, procedures and techniques, audit documents, regulations and other applicable requirements, etc.).

4.2.2 Personnel must have participated in at least two full audits, from preparation to final conclusions, within the past three years.

4.2.3 Staff must be able to benefit from a professional training programme.

4.2.4 Staff must have the required level of expertise with respect to the processing activities subject to the code and a thorough knowledge of data protection issues relevant to the specific area of the code.

4.2.5 Staff must have received specific training on the protection of personal data.

4.2.6 Staff with a legal profile must hold at least a master's degree or an equivalent degree in the field of law.

4.2.7 Staff with a legal profile must have at least two years of professional experience in the field of personal data protection (eg advice, litigation, etc.).

4.2.8 Staff with a technical profile hold at least a bachelor's degree or equivalent in the field of computing, information systems or cybersecurity.

4.2.9 Staff with a technical profile have received a minimum of two days' training on the useful reference systems for information systems security management (regulations, standards, methods, best practices, risk management, etc.).

4.2.10 Staff with a technical profile have at least two years' experience in the field of information systems security.

5. Requirements for inspection body procedures

Explicative note :

These requirements aim to guarantee that the control activities and missions carried out by the control body are regular, complete and transparent for the adherent to the code of conduct.

The control procedure can be designed in different ways, such as random and unannounced audits, annual inspections,

regular reporting and the use of questionnaires.

The monitoring procedure implemented by the monitoring body must comply with the framework established by the code of conduct.

5.1 The monitoring body shall demonstrate that the monitoring procedure determines the skills necessary to perform the assignment and ensures that personnel have the skills required to perform the monitoring assignment.

5.2 The inspection body must demonstrate that the inspection procedure includes a staff commitment to respect the principles of ethics, independence, impartial presentation of results and the use of a methodical approach.

5.3 The inspection body must demonstrate that the procedure provides for regular checks, carried out in an independent manner, which allow:

- to assess the eligibility of data controllers and/or subcontractors to adhere to the code,
- to monitor compliance with the code after joining, and
- to assess the proper functioning of the various mechanisms provided for by the code.

5.4 The control body must demonstrate that it has set up a control program taking into account elements such as the complexity of the processing and the risks associated with it, the number of members of the code, the geographical scope of the code and complaints received.

5.5 The inspection body shall demonstrate that the inspection procedure guarantees the integrity and traceability of evidence when collecting the necessary information.

5.6 The auditing body shall demonstrate that audit results and conclusions are disclosed and explained to adherents of the audited code within a reasonable time.

During an inspection, the written or oral remarks made by a member upon receipt of the findings and conclusions are listed in the report.

6. Complaint Handling Requirements

Explicative note :

The oversight body puts in place procedures for the impartial and objective handling of complaints about breaches of the code or the manner in which the code is applied by an adherent. These procedures are transparent and public to all.

The complaint handling procedure established by the regulatory body makes it possible to deal with complaints from a member

of the code or from any person who can demonstrate a legitimate interest. The handling of complaints must be subject to the allocation of sufficient resources and the staff involved must demonstrate sufficient knowledge and impartiality.

This procedure is also based on the applicable code of conduct.

6.1 The Oversight Body establishes a procedure to receive, manage and process complaints. The inspection body must demonstrate that this procedure is impartial and transparent.

6.2 This procedure must be understandable and easily accessible by all public, including the persons concerned and the adherents to the code.

6.3 The Oversight Body shall ensure that all complaints are dealt with and shall provide the Complainant with reports on the progress of the procedure or its outcome within a reasonable period, for example three months, of receipt of the complaint. The time limit for resolving the complaint may be extended for a reasonable period of time if necessary, taking into account the complexity of the complaint. The regulatory body shall inform the complainant of this extension within three months of receipt of the complaint, stating the reasons for the extension of the deadline.

6.4 The Oversight Body keeps a record of the handling of all complaints received.

The inspection body shall keep this register available to the inspection authority, which may access it at any time.

6.5 The Oversight Body shall make such decisions, or general information relating thereto, publicly available, in accordance with its complaints procedure.

This general information may include, but is not limited to, general statistical information regarding the number and type of complaints/violations and the resolutions/corrective measures issued. This general information must include information relating to the sanctions which led to the suspension or the exclusion of a member.

7. Supervisory Authority Information Requirements

Explicative note :

These requirements detail the information that a monitoring body must regularly communicate to the monitoring authority.

7.1 The inspection body compiles in a single document the summary of all the actions taken. This document is available to the supervisory authority, which can access it at any time.

7.2 The control body informs the control authority, without delay and in writing, of any substantial modification (in particular of structure or organization) likely to call into question its independence, its expertise and the absence of any conflict of interests.

'interests.

7.3 The monitoring body informs the monitoring authority, in writing, when a binding measure is taken against one of the members of the code of conduct. This information includes a presentation of the reasons justifying this measure.

The frequency of communications is based on several criteria, including the seriousness of the violation and the action taken.

7.4 The monitoring body informs the monitoring authority, without delay and in writing, as soon as the membership of a member of the code of conduct is suspended. This information includes a presentation of the reasons justifying this measure.

7.5 The monitoring body informs the monitoring authority, without delay and in writing, as soon as a member is excluded from the code of conduct. This information includes a presentation of the reasons justifying this measure.

8. Requirements for review mechanisms

Explicative note :

The code holder can decide to modify or extend the scope of the code and/or its content. In this case, control bodies are involved in this process: they play a key role in contributing to the updating of the code in accordance with the review mechanisms provided for by the code of conduct.

8.1 The inspection body contributes to the review and/or modifications of the code decided by the code holder.

8.2 The control organization must provide procedures allowing to integrate and implement the control of the changes decided by the codeholder.

8.3 The Overseeing Body also provides the Codeholder with a periodic report on the operation of the Code.

9. Legal status requirements

9.1 Inspection body requirements

9.1.1 The inspection body is established in the European Union.

9.1.2 The Monitoring Body is accountable to the Monitoring Authority for all its actions and decisions related to its activities.

9.1.3 The inspection body has sufficient financial, human and material resources and procedures to ensure the continuity of its inspection activities throughout the duration of the accreditation.

9.2 Subcontract Management Requirements

Explicative note :

The objective of these requirements is to guarantee compliance with this accreditation reference system when the inspection

body uses the services of a subcontractor for the performance of its inspection missions.

9.2.1 The monitoring body establishes a contract or other legal act under European Union law, linking it to the processor so that all tasks subcontracted comply with the GDPR.

The use of subcontracting does not lead to a delegation of responsibility: in all cases, the control body remains responsible for the control of the code of conduct before the control authority.

9.2.2 The control body ensures that any subcontractor meets the requirements of this reference system, in particular with regard to independence, the absence of conflict of interest and expertise.

9.2.3 The control body provides for the insertion of a special clause in the contract established with the subcontractor(s) in order to guarantee the confidentiality of personal data which could, if necessary, be brought to the attention of the subcontractor as part of the control.

10. Requirements for Sanctions and Corrective Measures Decided by Overseeing Body

10.1 The inspection body applies the corrective measures and sanctions provided for in the code of conduct.

10.2 The monitoring body must ensure that, in accordance with the code of conduct, the rights of the member are respected when the body requests the application of corrective measures or pronounces sanctions.

The president,

M. L. Denis