

Athens, 06-08-2020 Prot. No.: G/EX/5512/06-08-2020 PERSONAL DATA PROTECTION AUTHORITY DUE TO 26/2020 The Personal Data Protection Authority (hereinafter, the Authority) met , at the invitation of its President, in a regular meeting on 5-8-2020, following the meeting from 22-7-2020, in order to examine the matter described in the history of this present. The President, Konstantinos Menudakos, and the regular members Spyridon Vlachopoulos, Konstantinos Lambrinoudakis, as rapporteur, and Charalambos Anthopoulos, also as rapporteur, were present. The meeting was also attended, by order of the President, without the right to vote, the specialist scientists Fotini Karvela, legal auditor, Konstantinos Limniotis, IT auditor, Efrosyne Siougle, IT auditor and Eumorfia-Iosifina Tsakiridou, legal auditor, as assistant speakers, as well as Georgia Paleologu, an employee of the Department of Administrative Affairs, as secretary. The Authority took into account the following: The Authority, with Decision 9/2020, decided – in accordance with article 57 par. 1 item. p' of the General Data Protection Regulation (hereinafter, GDPR) – the drawing up of a plan that describes the requirements for the accreditation of monitoring bodies, as defined in article 41 of the GDPR, related to a code of conduct for which the Authority is responsible under with article 55 of the GDPR. In order to finalize these requirements, the Authority, in accordance with Article 41 para. 3 of the GDPR, applied the consistency mechanism referred to in Article 63 of the GDPR by submitting the draft of the requirements for approval to the European Data Protection Board (hereinafter, the Council) , as provided for in article 64 par. 1 item c' of the GDPR. The 1 Council, following a written procedure (written procedure), which is provided for in article 24 par. 3 of the internal Regulation and which was completed on July 23, 2020, issued opinion 20/2020 regarding the said plan of the Authority based on article 64 par. 3 of the GDPR. With this opinion, which was sent to the Authority electronically on July 29, 2020, the Council requested the Authority to amend the plan in question based on the recommendations included in it for the coherent implementation of the accreditation of the bodies monitoring codes of ethics. The Authority, after hearing the rapporteurs and the assistant rapporteurs, who then left, and after a thorough discussion, DECIDED IN ACCORDANCE WITH THE LAW 1. According to Article 9 of Law 4624/2019, which aims, – between others, - taking measures to implement the GDPR, the supervision of the implementation of the provisions of the GDPR in the Greek Territory is exercised by the Authority. 2. According to article 15 paragraph 10 of Law 4624/2019 "The regulatory acts of the Authority, for which it is not foreseen to be published in the Government Gazette, are published on the website of the Authority". 3. Pursuant to Article 41 para. 3 of the GDPR, the competent supervisory authority submits the draft accreditation requirements of the monitoring body to the Council in accordance with the consistency mechanism referred to in Article 63 of the GDPR. Furthermore, according to

article 64 paragraph 1 of the GDPR, "The Council shall issue an opinion whenever a competent supervisory authority intends to adopt any of the following measures. For this purpose, the competent supervisory authority shall announce the draft decision to the Council, when: (...) c) it aims to approve the requirements for the accreditation of a body in accordance with Article 41 paragraph 3 (...)." According to article 64 paragraph 3 of the GDPR, "In the cases referred to in paragraphs 1 and 2, the Data Protection Board issues an opinion on the subject submitted to it, if it has not already issued an opinion on the same subject. This opinion is issued within a period of eight weeks<sup>2</sup> by a simple majority of the members of the Data Protection Board (...)". Furthermore, according to article 64 paragraph 7 of the GDPR, "the competent supervisory authority referred to in paragraph 1 shall take particular account of the opinion of the Data Protection Board and, within two weeks of receiving the opinion, notify the President of the Data Protection Board by electronic means whether to maintain or amend the draft decision and, where appropriate, the amended draft decision, using a standard format".

4. In view of the above, the Authority, after taking into account and considering the recommendations, including the encouragements, of the Council's opinion 20/2020, decided unanimously that all the recommendations of the said opinion should be accepted, that the necessary changes should be made to draft of the accreditation requirements that it had initially submitted to the Council and to communicate to the Council an amended draft within the aforementioned deadline.

5. For this purpose, the necessary changes to fulfill all the recommendations and encouragements of the Council's opinion 20/2020 were carried out on the draft of the accreditation requirements drawn up with Decision No. 9/2020 of the Authority. The amended requirements are listed in the Annex to this decision. FOR THESE REASONS, the Authority unanimously decides to amend the plan of accreditation requirements for the bodies monitoring codes of ethics, based on the recommendations of the Council's opinion 20/2020, and to announce the amended plan to the Council, in accordance with article 64 par 7 of the GDPR. The amended plan, which is listed in the Appendix of this decision, will be made public by the Authority by publication on its website - in accordance with article 57 par. 1 item. website of the GDPR and with article 15 par. 10 of Law 4624/2019 - after the completion of the said procedure.

3 The President The Secretary Constantinos Menudakos Georgia Palaiologou

4 APPENDIX Personal Data Protection Authority Requirements for accreditation of bodies monitoring codes of ethics Introduction Regulation (EU) 2016/679 for the protection of natural persons against the processing of personal data and for the free movement of data of these (General Data Protection Regulation - hereinafter, GDPR) has been in force since May 25, 2018. Codes of conduct are provided for in article 40 of the GDPR. They are drawn up by associations or other bodies representing categories of controllers or processors. They aim to

facilitate the effective implementation of the GDPR by regulating specific obligations of both controllers and processors, for specific areas of activity. As they are optional and not mandatory, the Personal Data Protection Authority (hereinafter, the Authority) clearly encourages their preparation in accordance with what is prescribed in Article 40 of the GDPR, in the sense that they may constitute a set of special rules/practices that contribute to compliance with the overall conditions for the legal processing of personal data set by the GDPR, taking into account the special characteristics of the various areas of processing

1. The draft of such a code is submitted to the Authority, which gives an opinion (in accordance with Article 40 par. 5 of the GDPR) whether the because code is GDPR compliant and approves it if it deems that it provides sufficient guarantees (whether it is original code or a modification or extension of already approved code). A code of ethics approved by the Authority, as long as it is followed by a controller or processors, may be used as evidence of compliance with the obligations of the controller (art. 24 par. 3 GDPR) or as an element to 1 According to introductory paragraph 98 of the GDPR, "Associations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct, within the limits of this regulation, in order to facilitate the effective implementation of this regulation, taking taking into account the specific characteristics of the processing carried out in certain sectors and the particular needs of micro, small and medium-sized enterprises. In particular, such codes of conduct could regulate the obligations of controllers and processors, taking into account the risk that the processing could pose to the rights and freedoms of natural persons." 5 it is proven that the processor provides sufficient assurances in accordance with paragraphs 1 and 4 of article 28 (article 28 paragraph 5).

Pursuant to Article 41 para. 1 of the GDPR, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body (hereinafter, monitoring body) that has the appropriate level of expertise in relation to the subject matter of the code and is accredited to this purpose by the competent supervisory authority. Pursuant to Article 41 para. 2 of the GDPR, the monitoring body may be accredited to monitor compliance with a code of conduct if: a) it has demonstrated its independence and expertise in relation to subject of the code at the discretion of the Authority, b) has established procedures that allow it to assess the eligibility of relevant controllers and processors in order to apply the code, monitor their compliance with its provisions and periodically review the of its operation, c) has established procedures and structures to deal with complaints about violations of the code or about the way in which the code has been applied or is being applied by a controller or processors, and to make the procedures and structures these transparent to the data subjects and the general public, and d) proves, at the discretion of the Authority, that his duties and obligations do not entail a conflict of interest. Pursuant to Article

41 para. 3 of the GDPR, the competent supervisory authority submits the draft accreditation requirements of the monitoring body to the Data Protection Board (hereinafter, the Board) in accordance with the coherence mechanism referred to in Article 63 of the GDPR. The Council has issued guidelines 1/2019 regarding codes of conduct (hereinafter, codes) and monitoring bodies, in the light of the GDPR. This is the set of requirements for accreditation of the Authority's monitoring bodies, which are submitted to the Council in accordance with article 41 par. 3 of the GDPR. For their preparation, the above relevant text of the Council was also taken into account. It is noted that whenever a code of conduct is submitted for approval, the respective owner of the code (as defined below) will be required to demonstrate how their proposed monitoring body meets the requirements in question. Please note that monitoring body accreditation is only valid for a specific code: in case the same body wants to be accredited for another code, it needs to be re-accredited. 6 The accreditation of a monitoring body is carried out following a written application to the Authority. The accreditation application includes the following information: i) identification information of the monitoring body, ii) General Commercial Register number (if applicable), iii) VAT number, iv) seat of the monitoring body, v) contact details of the persons responsible for providing additional information about the accreditation application, vi) clarification of whether it is an internal or external monitoring body (as defined below). The application shall include evidence of the fulfillment of the requirements by providing relevant documents, as specified in said requirements. The body's accreditation by the Authority is valid for a period of five (5) years - unless the code itself provides for a shorter period. Claims can be reviewed before the five-year period has expired. Accreditation can be withdrawn at any time, provided the conditions described below are met. Three months before the expiry of the accreditation, the monitoring body must submit to the Authority a request for its renewal, quoting again all the evidence for the fulfillment of the requirements (with special reference to what is updated): the Authority may, in the context of examining the request renewal, to request further detailed information on the actions of the body in monitoring the compliance of the members of the code throughout the previous period. This does not concern, in the first place, the case of bodies monitoring codes of conduct of article 40 par. 3 of the GDPR, which can be observed by controllers and processors in order to provide the appropriate guarantees in the context of transfers of personal data to third countries or international organizations, in accordance with the conditions described in article 46 par. 2 item. eh. The above guidelines 1/2019 exclude this case. Basic definitions a) Code owner<sup>2</sup>: Association or organization that prepared the code and submitted it to the Authority b) Code member: any data controller (Article 4 para. 7 of the GDPR) or processor (Article 4 para. 8 of the GDPR) has join the code. Accreditation requirements The following apply to

both an external monitoring body and an internal monitoring body in relation to the code owner<sup>3</sup> (eg an ad hoc internal committee or a separate department of the code owner's organization, regardless of the fact that, in some In some cases, the requirements can be more easily satisfied for an external than for an internal. In specific cases of requirements that concern only an internal monitoring body, then special reference is made to this. 2 See also the definition of "code owner" in the guidelines lines 1/2019 of the ESPD 3 See also the guidelines 1/2019 of the ESPD, regarding the issue of external and internal monitoring bodies 7 1. General requirement of independence of the monitoring body (article 41, par. 2, item a' ) The monitoring body of a code must be independent from both the owner of the code and from each of its members. monitoring area should be understood as a set of formal rules and procedures for the mandate, responsibilities and operation of the monitoring body, which enable the monitoring body to monitor compliance with the code of conduct with complete autonomy, without direct or indirect influence or exercise pressure of any kind that might influence the decisions it takes. This means that the monitoring body cannot take orders to carry out its duties from members of the code, the profession, industry or sector where the code is to be applied, or from the owner of the code itself. Independence lies in four areas 4: i) Legal independence in decision-making processes, ii) Financial independence, iii) Organizational independence, iv) Independence in accountability. Independence – as specified below – must result from established clear rules and procedures in order to ensure that the monitoring body operates autonomously and without any pressure from the owner or members of the code, in accordance with the above. This independence must be demonstrated to the Authority. The monitoring body can be both external and internal in relation to the owner of the code, as long as the aforementioned independence is fully documented, as specified below. i) Legal and decision-making processes A) The monitoring body must be independent of the decision-making processes related to the monitoring of compliance with the code, from the code owner, the code members, but also from the sector more generally /branch the code is about. B) The monitoring body must demonstrate to the Authority that it acts fully independently in making decisions about compliance with the code. This can be demonstrated through clearly defined procedures for the selection of personnel to participate in both inspections/compliance checks and decision-making. The organization's defined procedures must ensure that its executives operate uninfluenced in the exercise of their duties both on a personal and professional level (e.g. 4 See also Opinion 9/2019 of the ESPD 8 or a department constitutes a wider organization in terms of professional collaborations). It should also be proven that the monitoring body, based on its legal status, will be legally able to issue fully independently enforceable decisions (e.g. its decisions should be immediately enforceable without requiring any other approval

or consultation , even if it is an internal monitoring body or if the body is external but of a group of companies/organisations).

For issuing decisions, it must be ensured that the body does not accept/expect orders/directions from anyone. This requirement applies not only to the monitoring body but also to its staff who will participate in the decision-making process.

Especially in the case of an internal monitoring body, additional safeguards regarding the independence of decision-making must be provided to the Authority, in order to ensure that the owner of the code to which it belongs does not in any way affect its independence (e.g. documents and recorded procedures that secure its independence in decision-making).

C) The monitoring body must not provide any other service to the members of the code and/or the owner of the code (e.g. consulting services regarding personal data protection issues), which could affect its independence in terms of making decisions regarding the compliance of the members of the code with it. It does not mean an internal monitoring body that is subordinate to a member of the code.

ii) Financial independence

A) The monitoring body must demonstrate to the Authority that it has the financial capacity and the required material resources in order to carry out its tasks in terms of monitoring compliance with the code. It must ensure long-term financial viability to ensure compliance with the code of conduct over time. For example, if a member of the code, who is being monitored by the body, may cease its financial contribution to the body in such a way that it becomes difficult or impossible for the body to carry out its duties of monitoring that member's compliance with the code, then financial independence of the body is not inferred<sup>5</sup>).

B) The monitoring body should have full autonomy in its financial management (that is, be able to make autonomous decisions of a financial nature - for example, how to allocate its budget) and this must be proven to the Authority.

<sup>5</sup> This does not in principle exclude the possibility of providing payment to the monitoring bodies, through e.g. contract, by the members of the code or the owner thereof, in order for the body to provide as a service the monitoring of compliance with the code. It also does not exclude the case of an internal independent monitoring body. In any case, however, it should be demonstrated that there is no financial dependence which could affect the impartiality of the monitoring body.

9 iii) Organizational independence

A) The monitoring body must have the necessary human and technical resources for the effective performance of its tasks. The monitoring body must demonstrate to the Authority that it has a sufficient number of adequately qualified staff to carry out its duties of monitoring compliance with the code, in such a way as to act independently of the members of the code and its owner. It must also demonstrate that it is fully independent in terms of the procedures it follows in relation to its staff (such as organizational chart, division of responsibilities, recruitment and assignment procedures, etc.) The monitoring body's staff must not be subject to any adverse consequence/sanction

because he performed his duties. B) In the case of an internal monitoring body, its organizational independence in relation to the wider body/organization to which it belongs must be documented, providing appropriate evidence (e.g. detailed description of overall organizational structure, existence of independent reporting/document management procedures and personnel management, information protection/confidentiality, separate branding/logo). In any case, the operation of the monitoring body must be independent of the operation of other accountability tools provided for in the GDPR that the controlled member of the code may use in the context of its compliance, as a controller or processor, with the GDPR . C) In the event that the monitoring body assigns to third parties (contractors/contractors) the process of monitoring compliance with the code, it is not exempted from any of its relevant obligations and responsibilities provided for in GDPR<sup>6</sup>. The obligations that apply to the monitoring body also apply to the contractor. The relevant delegation must be in writing and in such a way as to ensure that these third parties provide the same guarantees of proper monitoring of compliance with the code as those applicable to the monitoring body. The monitoring body must prove to the Authority that these guarantees have been obtained – such as: i) Relevant contracts/agreements in which the relevant obligations of confidentiality will be described, a precise description of the type of data that will exist and the contractor's commitments <sup>6</sup> This implies , among other things, that the Authority revokes the accreditation of the monitoring body if the contractor does not provide or no longer provides the appropriate guarantees or if the actions taken by the contractor violate the GDPR (see art. 41. par. 5 of the GDPR) . <sup>10</sup> can be processed as well as the purpose of the processing, as well as data security requirements. In the contracts there should be a specific reference to the fact that the contractor acts exclusively only on the basis of recorded orders of the monitoring body with the obligation to systematically inform the monitoring body of the findings/conclusions regarding the compliance of the code members with it based on the controls/ inspections it carries out, but also with the obligation to inform the monitoring body without delay in case any member of the code violates it. ii) The contractor will not be able to engage another subcontractor/contractor to in turn assign the code compliance monitoring. Decisions regarding compliance or non-compliance with the code are not made by the contractor but by the monitoring body. The monitoring body must demonstrate to the Authority that each contractor meets the requirements of its independence in relation to the members of the code and its owner, as well as the requirements of expertise and non-conflict of interest (by describing, and submitting to the Authority relevant evidence , how the monitoring body itself examined the fulfillment of these requirements). The monitoring body must ensure effective monitoring of the services provided by contracted contractors. iv) Accountability A) The monitoring body must provide the Authority with

evidence that it is able to demonstrate its independence (accountability) regarding its actions and decisions (e.g. by precisely describing the procedures it will follow and how these will be demonstrated, providing evidence of the appropriateness and adequacy of mechanisms to identify and mitigate risks to independence).

2. General requirement for non-existence of conflict of interest (Article 41, par. 2, letter d')

The monitoring body must have in place clear procedures which ensure that no natural or legal person who will carry out compliance monitoring tasks with the code will not be associated, directly or indirectly, with the audited code member, as well as with the owner of the code, with such a link that may lead to a conflict of interest.

11 The monitoring body must be able to demonstrate that it has considered potential conflicts of interest and has procedures in place to identify and effectively address them (e.g. full exclusion of employees reasonably suspected of having a conflict of interest, with documented assurance that monitoring of the corresponding code member will not be affected at all). These procedures must be continuous and binding on the staff of the monitoring body, who will have the obligation to inform the body in the event that they consider that any issue of conflict of interest arises. An example of a conflict of interest could be when the staff of the monitoring body investigates complaints against the organization in which they work or have worked in the past. Other examples of potential causes of conflicts of interest could include ownership, management, outsourcing and training. In any case, the monitoring body must ensure that its staff must not be in other employment such that, as a result of monitoring compliance with the code, they can gain some comparative advantage in relation to that other employment, so that to question his impartiality in making a decision.

3. General requirement for expertise in relation to the subject of the code (Article 41, par. 2, letter a')

The monitoring body must submit to the Authority evidence proving that it has the expertise to effectively monitor compliance with the code (e.g. for its staff relevant studies, as analyzed below, previous service, any relevant recognitions, etc.). Expertise relates to the subject matter (field) of the code, so the relevant requirements to be met may be specific, based on the field covered by the code: in this case, the code itself must set them. In addition, the risks of the processing activities covered by the code and the various interests involved should be considered. For related studies, in-depth understanding of data protection issues, experience with specific data processing activities, as well as sufficient operational experience of performing appropriate compliance checks (for example, with university degrees, certifications, related training programs etc. ).

The body should have the professional profile of its employees in terms of expertise, with appropriate documentation for each.

12

4. General requirement to establish procedures that allow assessment of the ability of code members to implement the code, the monitoring of their compliance with its provisions and the periodic review of its operation (article 41, par. 2, letter b')



The monitoring body must demonstrate to the Authority that it has and implements effective mechanisms to control the compliance of those responsible processors and code processors with appropriate review procedures, which may include audits, inspections, reporting and the use of self-monitoring reports or questionnaires. In addition, the monitoring body must demonstrate that it has a process for investigating, identifying and managing breaches of the code by its members as well as additional controls to ensure that appropriate action is taken to remedy those breaches as set out in the relevant code. In this context, it should describe in an official policy (e.g. approved by the General Manager of the monitoring body) at least the following:

- 1) Scheduling information of the controls it will carry out (e.g. whenever controls will be carried out, whether they will be sudden and, in the affirmative case, by what criteria will be decided their implementation, etc.), with appropriate documentation for the effectiveness of this scheduling, taking into account the periodic review of compliance that is required to be done, all members of the code, their geographical distribution, the characteristics of the sector covered by the code and the complaints that will be filed against members of the code.
- 2) Information on the control methodology to be followed (e.g. on-site inspections, interviews, questionnaires, etc.), as well as documentation of the effectiveness of the methodology (e.g. control points, how compliance with them will be established, etc.). The monitoring body must have specific and effective audit powers (eg it is expressly provided that auditees/code subjects are required to fully facilitate the audit of compliance with the code). Where the audit methodology adopted is based on a relevant audit standard, it should be reported and documented.
- 3) Information on how any violations found to comply with the code will be dealt with, i.e. how the monitoring body will impose the relevant sanctions provided for in the code or appropriate corrective measures will be implemented to ensure compliance. In cases where the audited code member must take corrective actions, information on how the body will verify their implementation.
- 4) Information on how audit reports/findings will be produced, what information they will contain and how they will be generally managed (e.g. members participating in an audit and writing the final report should be in a regime of secrecy and confidentiality, it should be clarified under which conditions the result of an audit is published or 13 communicated to third parties and, in such a case, what level of detail this will entail, etc.) In addition, the monitoring body must provide information that demonstrate that it has ad hoc regular procedures in place to monitor member compliance within a clearly defined timetable, and that it checks the eligibility of members prior to their participation in the code (such as procedures which provide for periodic audits to be scheduled);
5. General requirement to establish procedures and structures to deal with complaints about violations of the code or the way it has been or is being applied, and to make those procedures and structures

transparent to data subjects and the general public ( article 41, par. 2, letter c') The monitoring body must have absolutely transparent and understandable procedures regarding how someone can submit a relevant complaint, either against a member of the code or against the body itself. Furthermore, the monitoring body should demonstrate that it has the required resources to support these processes seamlessly. Also, in the context of the transparency of the relevant procedures, decisions taken by the monitoring body should be properly publicized (as specified below). The monitoring body must be able to demonstrate, at all times, that it has these procedures in writing (electronic or non-electronic) and that it has taken the required actions as described below. In particular, the monitoring body must satisfy the following:

A. Complaints against code members

a) The monitoring body must be able to demonstrate that the procedure for filing complaints against code members is easily accessible to the general public, fully understandable, transparent and fluent. The procedure must make clear the minimum elements required in order for a complaint not to be deemed vague or unsubstantiated.

b) Upon submitting the complaint, the body must inform the complainant that it has received the complaint, as well as inform him of the progress or outcome of the complaint within a specific date and no later than three months. The organization should document that it has the necessary procedures to enable a quick and effective control. The monitoring body must contact the complainant in order to give them the opportunity to further document the complaint or fill in missing information, if necessary. The said obligations of the body should be explicitly stated in the description of the complaint submission procedure.

c) The monitoring body should take appropriate effective actions in the event of a violation of the code by its member. Such actions, which the code should provide for, can be appropriate information, recommendation, special report to the management of the member of the code, decision of reprimand and/or warning in order to take immediate specific corrective measures, suspension of its adherence to the code or an exception to the code. These actions must be communicated to the complainant, but also to the code owner.

d) The monitoring body must keep a record of each complaint submitted to it, with all relevant information about the actions it took to investigate the complaint, including the final actions. The relevant records must be available to the Authority at all times.

e) The monitoring body must publicize the actions it undertook, as described in point c' above. This publication does not necessarily imply the publication of any audit finding or any decision of the body in its full form. The disclosure should concern those necessary elements that allow the general public to gain knowledge about compliance or non-membership of the code (eg a brief summary of a relevant decision), without details that are of a confidential nature. It is pointed out that the above point e' of case A respectively concerns not only actions of the body following a complaint but also actions following ex officio

controls which it carried out in the context of compliance monitoring. B. Complaints against the body itself a) The monitoring body must demonstrate that the procedure for submitting complaints/complaints against decisions it has taken or actions it has taken is easily accessible to the general public, fully understandable, transparent and fluent. The monitoring body must demonstrate that, in the event that it received such a report/complaint, it took appropriate action to investigate it and informed the complainant of the relevant report/complaint. In the event that, following examination of a relevant complaint/complaint, the institution takes a new action or modifies the relevant action it had taken (e.g. modification of a decision), then what is described above, in points c'-e' of case A. b) The monitoring body must inform the owner of the code of any such report/complaint submitted to him. c) In the event of a complaint being submitted to the Authority against a monitoring body, the latter shall fully facilitate the Authority in any relevant control that it will carry out. 6. General requirement to inform the competent supervisory authority about the body's actions in the event of a breach of the code by a member (Article 41, par. 4) or for a significant change in the body The monitoring body must have completely transparent and clear procedures regarding how with which it will inform the Authority of its actions and the degree of detail of the relevant information. Furthermore, the monitoring body must have correspondingly transparent and clear procedures regarding the way in which it will inform the Authority regarding substantial changes that take place to the body, which require its re-accreditation (e.g. any change affecting the body's ability to monitor to carry out his duties independently and effectively or will could call into question the independence, expertise and absence of any conflict of interest or to have an adverse effect on the overall of operation).

The above procedures must be made readily available to the Authority.

In particular, the monitoring body must satisfy the following:

a) The monitoring body must have a clear and transparent procedure in this regard with when he will inform the Authority of his actions, as well as the manner information. The notification to the Authority must always be in writing (electronic or non).

b) In case the monitoring body made a decision on suspension of a member of the code from joining it or for its exclusion from it

code, the Authority must be notified without delay at the initiative of the body.

In any such case, relevant evidence should be submitted to the Authority

which were taken into account in order for the monitoring body to issue the aforementioned

decision (eg information about the details of the offence, the finding or

audit findings and actions taken).

c) The monitoring body should at all times be able to have

to the Authority aggregated information of a statistical type regarding the actions on

which it has undertaken in order to check the compliance of members of the code with it,

as well as the relevant actions it has taken in the context of these controls.

16

To this end, it must have appropriate mechanisms for it without delay

export these statistics. In any case, if the Authority requests

more detailed information about a case (e.g. control, complaint examination, etc.)

which the body examined, the latter should immediately make available to the Authority

this information.

d) In a case where significant changes take place in the structure and

operation of the monitoring body, which may affect them

requirements under which it received accreditation, then the body should

inform the Authority without delay: to this end, he must prove that he has

implementation of the appropriate procedures for the timely recognition of the important

of these changes. In said procedures, the type of

of these changes which will mandate the obligation to inform the Authority

in order for the Authority to subsequently examine whether the

accreditation requirements.

7. General requirement for periodic review of its operation

code and for contributing to its revision (article 41, par.

2, item b')

The monitoring body must contribute to revisions of the code, according to requirement of the owner of the code, as well as to properly monitor the operation in order to be able to recognize if the code itself needs revision. For this purpose, the monitoring body must ensures that it has documented plans and procedures for its review operation of the code to ensure that the code remains relevant to members and is still subject to any changes in application and interpretation of the law or to any new technological developments that may have an impact on processing of the data by the members of the code or in the provisions of the code.

To this end, the monitoring body must satisfy the following:

a) The monitoring body must submit at regular intervals, and at least once a year, reporting to the code owner about its operation code, as well as any suggestions for revising it. Said report will it must contain information such as the dates of the audits, the scope of application them, the identity of the audited, the conclusions of the audits, whether they have filed a related complaint, etc. This does not remove the operator's obligation to promptly informs the owner of the code in the event that the operator finds that there should be an immediate revision of the code.

b) The body must have specific procedures in order to evaluate the operation of the code and be able to identify any need to revise it.

17

c) In case the revision of the code affects the body monitoring in any way (e.g. expanding the scope of control in which the operator must focus on), the operator should at all times be able to demonstrate that it has appropriate procedures in place to cope with

obligations, as well as that in general all accreditation requirements are met of. In case the code revision brings about a significant change to the institution which may affect the claims on the basis of which it was received accreditation, then what is stated above in point d of it shall apply proportionally claim no. 6.

General requirement regarding the legal status of the organization (s in relation to what is prescribed in particular in article 41 par. 4 but and in article 83, par. 4, item c')

The monitoring entity (e.g. limited liability company, association, internal department of code owner's organization, etc.) must have the appropriate legal status in order to be able to exercise his duties in accordance with article 41 of the GDPR.

Since the monitoring body is independently responsible for processing during meaning of article 4 par. 7 of the GDPR, its accreditation does not necessarily mean and assessment of its compliance as a controller with the GDPR. According with the principle of accountability of the GDPR (Article 5 par. 2), the monitoring body has responsibility and is able to demonstrate compliance with the GDPR. In case during which, at any time, non-compliance of the body is established monitoring with the GDPR, the Authority may revoke its accreditation.

The requirements regarding the nature/entity of the body are as follows:

a) Although there is no specific condition for the legal status of the body, the latter must have detailed documentation in order to demonstrate that has a legal form which allows it to exercise the powers which are provided for in article 41 par. 4 of the GDPR, as well as that the Authority may imposes the relevant sanctions according to article 83 par. 4 item. c' of the GDPR.

b) The monitoring body must have a complete and up-to-date

its organizational chart. The internal monitoring body must have and description with its exact associations with the code owner (providing the guarantees of independence according to the above).

c) The main establishment of the monitoring body must be located within the EEA.

d) A detailed, complete and updated list of legal entities must be submitted representatives of the organization as well as a list of persons responsible for communication with the Authority.

The monitoring body must render the above elements fluently available to the Authority. All supporting documents must be submitted to the Authority by the institution in the Greek language (in case it is a translation, this

18

it should be official). If it is a code that has a cross-border nature, then it should also be submitted in English.

The Secretary

The President of the Authority

Konstantinos Menudakos

Paleologo Georgia

19

20

Title: Incorporation of the recommendations of the draft opinion of the European Council

Data Protection regarding the requirements of the Authority for the accreditation of bodies monitoring codes of ethics

The Authority, with Decision 26/2020, modified the draft of the accreditation requirements for code of conduct monitoring bodies, based on its recommendations opinion 20/2020 of the Data Protection Council. The original plan, as it was formed by the Decision No. 9/2020 of the Authority, had been submitted to

Council within the framework of the coherence mechanism of the General Regulation

Data Protection (GDPR). With Decision 26/2020 it was decided

communication of the amended draft accreditation requirements to the Council;

in accordance with article 64 par. 7 of the GDPR. The amended plan will

be made public by the Authority by publication on its website – according to

with article 57 par. 1 item website of the GDPR and with article 15 par. 10 thereof

Law 4624/2019 - after the completion of said procedure.

21

22