Accreditation requirements of code of conduct monitoring bodies under Article 41 of the General Data Protection Regulation

Hungary

Table of contents

1055 Budapest
Falk Miksa utca 9-11.
Tel.: +36 1 391-1400
Fax: +36 1 391-1410
ugyfelszolgalat@naih.hu
www.naih.hu

1. Introduction

According to Article 41 (1) of the Regulation 2016/679 (EU) 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, hereafter: GDPR) the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

According to Section 38 para. (2a) of the Act CXII of 2011 on Informational Self-Determination and Freedom of Information (hereafter: Privacy Act), for natural persons and legal entities under the jurisdiction of Hungary, the tasks and powers specified in the General Data Protection Regulation for the supervisory authority shall be exercised by the National Authority for Data Protection and Freedom of Information (Nemzeti Adatvédelmi és Információszabadság Hatóság, hereafter: NAIH) according to the provisions of the GDPR and of the Privacy Act.

Article 41 para. (2) of the GDPR allows code owners to put forward proposals for their code monitoring body in order to gain accreditation by the competent supervisory authority. Under this Article the monitoring body must:

a) demonstrate its *independence* and *expertise* in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;
b) establish *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;
c) establish *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
d) demonstrate to the satisfaction of the competent supervisory authority that its tasks and duties do *not result in a conflict of interests*.

Pursuant to the aforementioned provisions of the GDPR and the Privacy Act the NAIH publishes the following accreditation requirements of code of conduct monitoring bodies. These accreditation requirements should be read alongside the EDPB Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under the GDPR.[1]

2. Procedural provisions and fees for application

According to Section 64/A para. (1) point b) of the Privacy Act the NAIH shall conduct a procedure for the authorisation of data processing if an application for the accreditation of the monitoring activity referred to in Article 41 of the GDPR is submitted.

In addition to the provisions laid down in Act CL of 2016 on the Code of General Administrative Procedure, the application shall contain the data demonstrating that the conditions specified in Article 41 para. (2) of the GDPR and in the accreditation requirements issued by the NAIH are complied with.

[1] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf

According to Section 64/B of the Privacy Act an administrative service fee, as determined in Decree 25/2018 (IX. 3.) of the Minister of Justice (hereafter: Ministerial Decree), shall be paid for a procedure for the authorisation of data processing. Pursuant to Section 1 point b) of the Ministerial Decree the amount of the fee is 530.000 HUF for an application for the accreditation of the monitoring activity referred to in Article 41 of the GDPR. The fee must be paid in advance to the NAIH's following bank account at the Hungarian State Treasury: 10032000-00319425-00000000.

According to Section 64/C of the Privacy Act the administrative time limit in authority procedures for the authorisation of data processing shall be one hundred and eighty days for applications for the accreditation of the monitoring activity referred to in Article 41 of the GDPR. If there is a cross-border matter regarding the accreditation procedure, the NAIH shall suspend the accreditation procedure for the cooperation procedure referred to in Article 60 para. (3) to (5) and the consistency mechanism referred to in Articles 63 to 66 of the GDPR with the proviso that the NAIH shall implement the procedural acts necessary in the cooperation procedure and in the consistency mechanism also during the period of suspension.

Where an application for the accreditation of the monitoring activity is submitted, the NAIH, in the authority procedure, may invite the applicant, on as many occasions as necessary, to make a statement with respect to amending or supplementing the application or the drafts included in it so that approval or authorisation can be granted.

An accreditation term will be initially set at three years at which time there would be a review to ensure that the monitoring body still meets the accreditation requirements. This term is without prejudice to the possibility for the owners of the code of conduct to provide for a shorter duration of the monitoring body in the code itself.

The NAIH shall issue a resolution in an official administrative procedure according to the relevant provisions of Act CL of 2016 on the Code of General Administrative Procedure about the accreditation of the monitoring body. The term of accreditation shall be set out in this resolution. If the term set out in the resolution expires without an application of renewal, the accreditation of the monitoring body ceases automatically.

With a view to verifying that the monitoring body complies with the accreditation requirements and carries out its monitoring functions in accordance with the GDPR, the NAIH reserves the right to initiate a review of the accreditation prior to expiry of the relevant term where it becomes aware of supervening risk factors or elements that may affect compliance by the monitoring body with the said requirements or monitoring obligations or else the conformity with the GPDR of the measures adopted by the monitoring body.

The monitoring body shall be accredited for the duration for which the accreditation is granted, except where the review carried out by the NAIH establishes that the monitoring body does no longer meet the accreditation requirements or is not capable to fulfil its monitoring obligations or else that the measures it has adopted are in breach of the GDPR.

An application to renew the accreditation may be sent to the NAIH up to one hundred and eighty days in advance of the expiration deadline to comply the time limit set in Section 64/C of the Privacy Act. The rules for the administrative service fee shall be applied for the procedure of renewal as set out in Section 1 point b) of the Ministerial Decree.

If the accreditation term expires without an application of renewal, the monitoring body cannot exercise its powers set out in the GDPR, the Privacy Act and these accreditation requirements any more.

The introduction of a new or additional monitoring body for a code of conduct will require the new body to be assessed in line with the accreditation requirements. The rules for the administrative service fee shall be applied for this procedure of accreditation as set out in Section 1 point b) of the Ministerial Decree.

As the specificities of the sector(s) covered by the code of conduct are taken into due account by the NAIH, a separate accreditation application will have to be submitted to the NAIH to enable a monitoring body that is accredited to monitor a given code to carry out monitoring functions with regard to a different code. The rules for the administrative service fee shall be applied for this procedure of accreditation as set out in Section 1 point b) of the Ministerial Decree.

3. Content requirements of the application

Applications for monitoring body accreditation must be submitted with all supporting documents to the NAIH. The following availabilities can be used for the official submission and correspondence:

by mail: H-1363 Budapest, Pf.: 9.
by official electronic gateway: short name: NAIH, KRID: 429616918

The application shall be in Hungarian and supported by the documents providing evidence of the fulfilment of the said requirements. The application shall include the following information:

a) Information identifying the applicant; if the applicant is a society, association, foundation or other organization, information identifying the legal representative and any person responsible for adopting the decisions on monitoring activities that produce external impacts;
b) The Tax ID / VAT Registration Number and, where appropriate with regard to registered companies, the Company Registration Number;
c) The applicant's residence, or the registered office in case the applicant is a company, association, foundation or other organization, which in either case shall be in the European Economic Area;
d) The articles of incorporation and the bylaws as for companies, associations, foundations and other organizations;
e) Number and roles of the employees;
f) The contact details to be used for any communications relating to the accreditation application;
g) Specification of the type of monitoring body (i.e., whether it is internal or external);
h) Specification of the code of conduct in whose respect accreditation is being sought;
i) Designation of the categories of controllers, processors and sectors for which the monitoring body is responsible;
j) Determination of the territorial scope in which the monitoring body exercises its monitoring activity, including the national or transnational scope of application of the code of conduct.

If more than one monitoring body is seeking accreditation for the code of conduct, in addition to demonstrating the fulfilment of the requirements specified in Article 41 para. 2 of the GDPR, the applicant must describe the competence and responsibility of the monitoring body seeking accreditation in the application subject to the code of conduct. Competences and responsibilities of the monitoring bodies must be distinguished. In this respect, the application shall contain a list or guide on the distribution of their competences regarding the monitoring activity and indicating which monitoring body is responsible for which code members. The application must also describe the necessary structures, business processes and other organisational measures.

The accreditation application shall be accompanied by all the appropriate documents providing evidence that the accreditation requirements set out in the following points of this accreditation requirements are fulfilled.

In the accreditation procedure the monitoring body must demonstrate its ability to exercise its monitoring activities in accordance with the requirements of Article 40, 41 GDPR and these accreditation requirements.

4. Legal status

The monitoring body must be a legal entity with a registered office or, if a natural person, have their headquarters or domicile, to exercise the professional activity as a monitoring body in the European Economic Area.

The monitoring can be carried out by an external body in relation to the code owner (external monitoring body) or as an internal body of the code owner (internal monitoring body). By internal monitoring bodies further measures shall be taken in order to guarantee organisational separation within the code owner's structure (see point 5 for further details).

If the monitoring body is a natural person than it must prove that it has the necessary human, financial and other resources and procedures to completely fulfil its monitoring body responsibilities. Especially, it must be ensured, that in the event of an unforeseen event leading to a sudden, temporary or permanent loss of the monitoring body, the monitoring activities may continue uninterrupted.

5. Independence

In accordance with Article 41 para. (2) point a) of the GDPR, the monitoring body must demonstrate that its independence from the code members, the code owner and from the professional industry and sectoral subject matter of the code of conduct is ensured at all times. In this respect, it must also demonstrate that it has implemented the appropriate procedures and structures to effectively manage any risks with respect to its independence. Independence is only possible if impartiality, objectivity and integrity are guaranteed.

Independence includes legal, economic, personal and factual aspects. In accordance with the following provisions, the monitoring body must take appropriate measures, to counter any direct or indirect interference, whether commercial, financial or otherwise, which could endanger or jeopardise the impartiality of the monitoring body.

The monitoring body must not receive instructions regarding the performance of its tasks and must not be influenced directly or indirectly in its performance of such. In addition, the monitoring body must not be penalised for the performance of its tasks by neither the code owner nor the code members.

5.1. Independence of organisational structure

Internal monitoring bodies cannot be set up within code members. The monitoring can be carried out by an internal body of the code owner, though in this case it must demonstrate its independence regarding its duties: evidence must be provided through documented rules and procedures.

In particular, it must be demonstrated that the internal monitoring body is structurally separate from the other areas of the code owner up to and including the level below the senior management. In this respect, the monitoring body must have its own personnel, and must be separate from the other areas of the code owner in terms of its functions, accountability and reporting system. The internal monitoring body must have separate management from other areas of the organisation. The internal monitoring body reports directly to its highest management level. Furthermore, it must be ensured that neither the code owner nor the code members exert any influence on the monitoring body.

Where the monitoring body is external to the code owner, it shall be demonstrated that the monitoring body does not provide the said code owner or the members of the code or the profession, industry or sector the code applies to with any product or service that may undermine its autonomy, independence, and impartiality or the actual discharge of its monitoring functions.

The monitoring body can demonstrate its organisational independence, for example, by the following documents:

- *Articles of incorporation and bylaws of the monitoring body and the code owner;*
- *Rules and procedures for membership, appointment, remuneration and terms of office of the monitoring body personnel in charge of taking decisions related to monitoring activities;*
- *Documents providing evidence of the business, financial, contractual or other relations between the monitoring body and the code owner or the association/organisation submitting the code.*

5.2. Independence of financing

The monitoring body shall demonstrate it has the financial resources required to effectively discharge its tasks and to meet its liabilities. The monitoring body must have the necessary financial resources to ensure its long-term financial stability. In addition, should one or more code members exit the code of conduct, this must not jeopardise the financing of the monitoring body.

The monitoring body shall be able to manage its financial resources autonomously and independently, without any interference, pressure or control by the code owner, the members of the code or the profession, industry or sector the code applies to.

The monitoring body shall demonstrate that its financing mechanisms are such as not to undermine the autonomy, independence and impartiality of its monitoring functions and that they are duly accounted for. If the monitoring body is an internal body of the code owner, a specific budget has to be allocated.

The monitoring body can demonstrate its financial independence, for example, by the following documents:

- *Submission of its sources of financing to the NAIH as evidence of sufficient financial resources;*
- *Financial risk assessment arising from its activities;*
- *Internal procedures to avoid preclusive circumstances and make adequate provisions for residual risks to mitigate the liabilities arising from its activities (e.g. conclusion of a financial loss liability insurance, creation of reserves).*

5.3. Independence of personnel

The monitoring body shall demonstrate it has the appropriate human, technical and logistical resources to effectively perform its monitoring tasks. Such resources shall enable the monitoring body to perform its monitoring functions in a fully autonomous, independent and impartial manner.

The resources should be proportionate to the expected number and size of code members, as well as the complexity or degree or risk of the relevant data processing. Personnel of the monitoring body shall be responsible and shall retain authority for their decisions regarding the monitoring activities.

The monitoring body shall demonstrate it has experienced staff. That staff shall be in any case under the exclusive authority and direction of the monitoring body and subject to specific confidentiality duties in discharging their tasks. The monitoring body must have a sufficient number of sufficiently qualified persons (in-house personnel or external service providers) and ensure adequate remuneration for its employees.

The monitoring body must be responsible for its own personnel within the scope of its monitoring tasks, and must be entitled to take decisions on its own responsibility and without instructions. Such instructions should not be taken by the code owners and members within the scope of the code at stake.

Where the monitoring body relies on external staff and sub-contractors that have been specifically delegated with carrying out individual monitoring activities arrangements shall be in place so as to ensure that such staff and contractors have the required expertise, competencies and reliability with particular regard to the subject matter of the code. Activities entailing decision-making powers may not be delegated to whomsoever.

The monitoring body must have appropriate and sufficient technical resources to perform its tasks competently and securely. The adequacy of the technical resources must be checked on a continuous basis.

The monitoring body can demonstrate its independence of personnel, for example, by the following documents:

- *Specific organisational and management models and operational procedures ensuring that the management and operation of the monitoring body works separately from the code owner and code members;*
- *Documented procedures and organisational rules to recruit and rely on external staff and sub-contractors;*
- *Documented procedures and organisational rules to ensure expertise, competencies and reliability of external staff and sub-contractors;*
- *Contractual or other legal instruments detailing the respective responsibilities including confidentiality of processed data and information.*

5.4. Independence of decision-making processes

The monitoring body must be independent with respect to its decisions and actions. The monitoring body shall act independently in its choices and application of sanctions against a controller or processor adhering to the code.

Any 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. This independence ensures that the monitoring body is accountable for its decisions and actions.

The monitoring body can demonstrate its independence of decision-making and its accountability for its actions, for example, by the following documents:

- *Documentation of decision-making procedures;*
- *Documentation of appropriate role structures and reporting mechanism.*

- *Setting up policies to increase awareness among the staff about the governance structures and the procedures in place.*

6. Expertise

In accordance with Article 41 para. (2) point a) of the GDPR, the monitoring body must demonstrate expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority.

The monitoring body shall have the appropriate expertise to accurately and effectively carry out its monitoring functions by having regard to the specific code of conduct. The availability of the expertise of the staff shall be demonstrated in the following subjects:

a) Appropriate knowledge and experience in the field of data protection law;
b) Technical expertise in the area of data protection, if this is necessary regarding the code's scope;
c) In-depth knowledge in the subject matter of the code of conduct, the processing operations and related risks covered by them and the processes in this area;
d) In-depth knowledge and expertise in carrying out supervisory and control functions (for instance in the audit or quality control sectors);
e) Expertise should be subject of regular training activities by having regard to the developments in the applicable legislation and the technology deployed in the sector.

The personnel responsible for the monitoring activity must have legal and technical expertise and qualification, but not necessarily present in one person:

- Legal personnel must have at least a Master's degree (MA) or an equivalent degree in the field of law.
- Technical personnel must have at least a Bachelor's degree or an equivalent degree in the field of computer sciences or information systems.

Personnel responsible for the management of the monitoring body must have a professional qualification and relevant professional experience in law, technology and the area covered by the code of conduct, but not necessarily present in one person.

More detailed expertise requirements can be set out in the code of conduct itself and considered as part of the accreditation.

The monitoring body can demonstrate its expertise, for example, by the following evidences:

- *CVs of the staff, training certificates, university degrees, postgraduate of master's degrees, PhDs, other professional qualifications and relevant work experience;*
- *Publication of scientific papers and any other evidence of qualified professional, study or research experience in the relevant field;*
- *Documentation of the hiring process taking into account the requirements above.*

7. Procedures and structures established

According to Article 41 para. (2) point b) of the GDPR the monitoring body shall demonstrate that it has 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.

Such procedures shall be laid down by having regard to the categories of processed data, the complexity of the processing and the risks to data subjects, the type and (expected) number of code members, the geographical scope of application of the code, the complaints received and any established infringements. Monitoring bodies must establish the basis and scope of their activities prior to the start of their monitoring tasks to ensure transparency for the code members.

7.1. Verification of applications to join the code of conduct

The monitoring body shall have a procedure for application verification in which it shall assess whether the code member is able to implement the code of conduct. The established procedures of the monitoring body shall ensure that the applications to join the code of conduct by data controllers and data processors are handled within a reasonable timeframe.

7.2. Procedures for monitoring of compliance with the code of conduct

The monitoring body shall have established inspection procedures to monitor the compliance of code members with the code of conduct. The number of code members inspected on an annual basis must allow conclusions to be drawn as to the extent of the implementation of the code of conduct by the code members.

The monitoring body shall have a specific control methodology with particular regard to 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.

The control procedure shall ensure that each inspection is prepared and framed by instructions including, in particular, details on the scope of the inspection, the allocation of necessary time and adequate technological resources in the relation to the subject matter of the code. The inspection report is sent within a reasonable period of time to the inspected controller or processor with the reasons and supporting elements for each observation. The inspected code member is allowed to make its remarks upon receiving the findings and conclusions of the inspection.

The monitoring body has to adopt appropriate corrective measures and sanctions, including suspension or exclusion of the controller or processor concerned from the code, within a reasonable period in order to remedy infringements and violations of the code of conduct by the members and prevent their re-occurrence in accordance with the provisions made in the code for any breach of its rules.

The number and selection of the code members to be verified is based, for example, on the risk content of the data processing, complaints, the number of code members, the territorial scope of the code of conduct and changes in the relevant data protection laws. The verification procedure can take place via surveys and (additionally) on site. In addition to the routine monitoring during the rotation tests, event-related checks may be also carried out.

The code members shall ensure their full cooperation in order to enable carrying out effective controls of the monitoring body.

The procedures may envisage publication of reports concerning the controls performed or else regular or summary reports on the activities carried out by the monitoring body and the relevant findings.

7.3. Verification of suitability of the code of conduct

The monitoring body shall contribute to the review of the code of conduct, which may include a regular or event-related conceptual review, to ensure that the codes of conduct are practicable, sufficiently precise and clearly written, fulfil the regulatory requirements and are accepted in practice. New technological developments which may have an impact upon data processing carried out or the provisions of the code should be also taken into account for the review of the code.

Should the monitoring body ascertain any defects, it shall notify the code owner and recommend a review of the relevant regulation(s) within the framework of the evaluation anticipated as part of the codes of conduct. The information may, as far as possible, already contain proposals to eliminate the defects identified. The updating of the code of conduct is the responsibility of the code owner.

7.4. Procedures to maintain confidentiality

The monitoring body shall have documented procedures to maintain appropriate confidentially. All information received by the monitoring body as part of its monitoring activities, in particular via the code members or their contractual partners (e.g. customers), including the sources of such information, must be treated as confidential, unless the monitoring body is required to disclose such by law or is authorised to do so under the contract.

The monitoring body is compelled to disclose confidential information to the NAIH in order to help carrying out its supervisory activities.

The monitoring body must demonstrate that it has documented procedures to ensure confidentiality through third parties acting on its behalf.

7.5. Providing regular and event-related information about monitoring activity to the supervisory authority

In accordance with Article 41 para. (4) of the GDPR, the monitoring body must inform the NAIH in writing, at regular intervals and at least once a year, regarding the measures taken in cases of infringement of the code by code members and the reasons for taking them. This can be in the form of a summary.

The monitoring body shall demonstrate it has a procedure in place to inform the NAIH, without undue delay, of the measures taken and the underlying reasons in case of infringements that entail suspension or exclusion of the relevant member from the code of conduct.

The monitoring body shall notify the NAIH in writing of any changes that could substantially affect the monitoring activities of the monitoring body.

The monitoring body shall inform the NAIH, without undue delay, of any substantial change to the monitoring body (particularly related to structure or organisation), 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.

8. Complaints handling mechanisms

According to Article 41 para. (2) point c) of the GDPR the monitoring body shall have 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.

8.1. Complaints by data subjects and other affected entities

The complaints handling mechanism shall ensure that a data subject or any person who can demonstrate a legitimate interest in the same way has the right to lodge a complaint by the monitoring body by sending an application including a short description of the facts and the alleged violation.

These mechanisms shall function without prejudice to data subjects' right to lodge a complaint by the NAIH or bring a proceeding before judicial authorities under Articles 77 and 79 of the GDPR and Sections 22 and 23 of the Privacy Act.

The monitoring body shall demonstrate it has implemented an adequate framework of procedures and structures to receive, investigate and decide on complaints. Such procedures shall be transparent, easily understood and easily accessible to the public as well as adequately resourced so as to ensure effective handling of complaints. The monitoring body can also make publicly available its decisions or information thereof.

The monitoring body shall have to demonstrate that it can take one or more corrective measures as laid down in the code of conduct, including sanctions, in case of infringements of its rules by the members so as to remedy those infringements and prevent their re-occurrence. The measures in question shall include suspension or exclusion of the relevant member from the code by taking account of the severity of the established infringements.

The complaints handling procedure shall provide that the monitoring body shall inform the complainant of the progress and outcome of his / her complaint within a reasonable timeframe. The time frame should not exceed 3 months. In any event, the monitoring body informs the data subject regularly. Every decision has to be properly justified.

8.2. Transparency of the complaints handling procedure

The description of the complaint procedure must be published by both the monitoring body and the code members in a form that is generally and easily accessible to the public following a successful accreditation of the monitoring body.

The procedure is generally and easily accessible, for example, if:

- *It is published on the homepages of the monitoring body and the code members;*
- *There is an easily accessible template for complaints.*

8.3. Communication with the supervisory authority regarding complaints

The monitoring body shall set up and regularly update a register of all the complaints and the corrective measures taken, including sanctions, which the NAIH may access at any time.

9. Conflict of interest

In accordance with Article 41 para. (2) point d) of the GDPR, the monitoring body may be accredited to monitor compliance with a code of conduct where that body has demonstrated to the satisfaction of the NAIH that its tasks and duties do not result in a conflict of interests.

9.1. Processes to avoid conflict of interest

To avoid conflicts of interest, the monitoring body must, in particular, be free of external (direct or indirect) influence and, therefore, it shall not seek nor take any instructions from any person or organisation.

The monitoring body should be appropriately protected from any sort of sanctions or interference by the code owner, other relevant bodies, or members of the code, as a consequence of the fulfilment of its tasks, regardless of its internal or external nature.

The monitoring body shall have a process for avoiding and managing conflicts of interest related to its personnel or the monitoring body itself. The procedures and measures in place to avoid conflict of interest ensure that the monitoring body shall refrain from any action incompatible with its tasks and duties. Employees of the monitoring body shall report in writing any potential conflicts of interest or threats to independence.

The monitoring body should have its own staff chosen by them or other body independent of the code and that the staff at stake should be subject to the exclusive direction of those bodies only.

The monitoring body may not accept any services from the code owner, code members or other third parties that could jeopardise their independence or promote conflicts of interest. In principle, there are no conflicts of interest if the services are non-supervisory, purely administrative or organisational assistance or support activities which have no influence on the impartiality of the monitoring body and which, in particular, do not influence the decisions of the monitoring body, e.g. IT support, payroll, clerical work, cleaning services, etc.

The monitoring body can demonstrate the mitigation of conflict of interest, for instance by:

- *Procedures in place to select the personnel empowered to decide;*
- *Respective remuneration arrangements;*
- *Conditions for renewal of appointment upon expiry of the personnel's terms of office.*

9.2. Outsourcing of individual activities and processes

Individual activities and processes of the monitoring activity can be outsourced to external service providers, provided that the monitoring body can prove that it has documented procedures and structures and it does not endanger its independency and does not give ground to any conflict of interest.

The monitoring body shall prove that by outsourcing its activities the requirements for the monitoring body are essentially fulfilled in the same way by the external service provider. Outsourcing does not result in a delegation of responsibility for the monitoring and, in any event, the monitoring body remains ultimately responsible to the NAIH as competent supervisory authority for monitoring.

If the monitoring body intends to outsource individual activities and processes of the monitoring activity to an external service provider, the monitoring body must have a documented outsourcing procedure. In this context the monitoring body shall have a legally binding, enforceable written

agreement with each provider of outsourced services. The agreement shall guarantee the expertise and independence of the personnel employed by the contractor, and assure of impartiality, confidentiality and no conflicts of interest.

In the event of an intended or anticipated termination of the outsourcing agreement, the monitoring body shall ensure the continuity and quality of the outsourced activities and processes after termination.

The monitoring body can demonstrate its outsourcing activities, for example, by the following documents:

- *Template of processor agreement used for outsourced activities.*
- *Any relevant document which testifies service provider's independence, expertise and the absence of conflict of interests related to the outsourced activity.*
- *Template of data protection and / or confidentiality agreement.*