Requirements for accreditation of a monitoring body for code of conduct under Article 41 GDPR in conjunction with Article 57 para. 1 lit. p 1. alt. GDPR

23 September 2020

1 Application requirements 2

2 Requirements for monitoring bodies 3

2.1 General requirements 3

2.2 Independence 4

2.3 Expertise 6

2.4 Conflicts of interest 7

2.5 Outsourcing 7

2.6 Procedures and structures established by the monitoring body 8

3 Powers 11

3.1 Knowledge of the contact details and contact persons of the code member, and the responsible managing director 11

3.2 Powers of investigation 11

3.3 Competence to act 12

4 Complaint procedure 12

4.1 Documentation of proof of an appropriate complaint procedure 12

4.2 Documentation of proof of a transparent complaint procedure 12

Annex 1: List of abbreviations / Glossary 13

A prerequisite for the accreditation of a monitoring body for code of conduct under Article 41 and Article 57 para. 1 lit. p 1. alt. GDPR is, in addition to the submission of an application, the fulfilment of the requirements set out in Article 41 para. 2 GDPR. The competent supervisory authority for the accreditation will examine the fulfilment of the requirements stated in Article 41 para. 2 GDPR based on the following accreditation requirements.

1 Application requirements

Accreditation requires a full written application to the supervisory body responsible for the monitoring body. Applications may also be submitted electronically, provided the legal requirements are met with respect to the competent supervisory authority. The written form also applies to any information attached to the application in the form of annexes. References to any potentially publicly available information are not possible.

The language of proceedings is German. If applications are submitted to the competent supervisory authority in a foreign language or if any submissions, evidence, certificates or other documents are presented, the competent supervisory authority may immediately request a translation of such. In justified cases, the submission of a certified translation or translation carried out by a public appointed or sworn interpreter or translator may be required.

The application shall include in particular the following information:

a) Name/company of the monitoring body, including identifiable address, telephone, email address;
b) Legal or authorised representative of the monitoring body, where applicable;
c) Contact person of the monitoring body within the context of the accreditation process and their contact details;
d) Number and roles of the employees;
e) General information on the monitoring body including organisation chart (with details of the company name and registered office) and the internal organisational structure and any relationships with superordinated, subordinated or same-level entities within the group or affiliated group organisations;
f) Designation of the code of conduct, the monitoring of which is the responsibility of the monitoring body seeking accreditation;
g) Designation of the categories of controllers, processors and sectors for which the monitoring body is responsible;
h) Determination of the territorial scope in which the monitoring body exercises its monitoring activity.

The application must contain the confirmation that, at the time of application and during the activity of the monitoring body:

a) No relationships exist between the monitoring body and one or several code member/s to minimise any risk arising from such (see no. 2.2.1) and
b) No personnel of the monitoring body who are assigned to any monitoring tasks are in any advisory relationship with the code members.

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 GDPR, the applicant must describe the competence and responsibility of the monitoring body seeking accreditation in the application in a transparent way. Competences and responsibilities of the monitoring bodies must be distinguished in such a way that the respective monitoring body and the competent supervisory authorities are both able to perform the tasks assigned

to them. In this respect, the application shall contain a list 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 competent supervisory authority must be notified without undue delay in writing of any changes during the application phase that may jeopardise eligibility or significantly impair the monitoring activities of the monitoring body.

2 Requirements for monitoring bodies

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 at all times. The following requirements essentially apply to both internal and external monitoring bodies.

Proof may be provided, for example, as follows:

1. Disclosure of the beneficial owners of the monitoring body (e.g. natural or legal persons who exercise a controlling influence over the monitoring body within the meaning of Section 290 para. 2 HGB (German Commercial Code));
2. Information on the decision-makers within the monitoring body;
3. Information on the funding of the monitoring body;
4. Submission of the documentation of the assessment of the risks arising from their activities with respect to the independence of the monitoring body;
5. Submission of the established principles of the monitoring activities e.g. in the form of instruction manuals and guidelines;
6. Submission of the documentation of the procedures and structures, in particular the structural and procedural business processes and other organisational measures.

2.1 General requirements

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.

If the monitoring body is a natural person, more stringent requirements exist to demonstrate the fulfilment of the accreditation requirements defined herein. In this case, the monitoring body must, in particular, prove that it has the necessary human resources and, 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.

The monitoring body must document the principles of its monitoring activities in writing. The procedures and structures of the monitoring body, in particular its structural and procedural business processes and other organisational measures, must be adequately documented. The monitoring body must ensure that it fulfils its tasks under Article 40 para. 4 and Article 41 para. 2 and 4 GDPR and is able to take effective measures in accordance with Article 41 para. 4 at all times.

2.2 Independence

In accordance with Article 41 para. 2 lit. a GDPR, the monitoring body must demonstrate that its independence from the code members, the code owner and from the profession, industry or sector to which the code applies is ensured at all times. In this respect, it must also demonstrate that it has implemented 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.

2.2.1 The independence of the monitoring body with respect to its legal form and decision making procedures

The legal form, duration and termination of the activity and other aspects of the implementation of the monitoring body shall enable the monitoring body to perform its tasks independently both by the code members and by the code owner. This includes the selection and application of measures and sanctions with respect to the code members. 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, it is the monitoring body that assumes responsibility for its activities and neither the code members nor the code owner must be penalised for the performance of monitoring body`s tasks. Rather, the monitoring body is to be protected against any dismissal or sanction, direct or indirect for the performance of its duties.

No legal, economic or other links between the monitoring body and the code members must exist that exceed the assurance of the financial independence or long-term financing set out in no. 2.2.2., unless the monitoring body can prove it has made reasonable provision to minimise any potential risk arising. Exceptions to this criterion are, in particular, purely administrative or organisational assistance or support activities which exert no influence on the independence of the monitoring body, and which exert no influence on the monitoring body's decisions (see also no. 2.4).

Internal monitoring bodies cannot be set up within code members. If the monitoring is carried out by an internal body of the code owner, e.g. in the form of an ad hoc committee or an independent internal body of the code owner, more stringent requirements are imposed to demonstrate independence. 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 (Chinese Walls) 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 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.

2.2.2 Independence of the monitoring body with respect to its financing

The monitoring body must have sufficient financial resources. Adequate resources depend on the number, size and complexity of the code members, the type, scope and extent of their activity as determined by the code of conduct and the risk content of the processing operations covered by the code of conduct. 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 submit its sources of financing to the competent supervisory authority as evidence of sufficient financial resources. The monitoring body shall ensure that financing is independent of the performance of its tasks, sanctions against individual code members and of the fact that individual code members belong to the code of conduct. In particular, in the event of financing through contributions from the code members, it must be ensured that the loss or exclusion of individual code members from the code of conduct shall not entail the immediate termination of the obligation to contribute.

To demonstrate adequate financial resources, the monitoring body must also assess the risks arising from its activities, implement internal procedures to avoid preclusive circumstances and make adequate provisions for residual risks.

2.2.3 Independence of the monitoring body in terms of personnel and other organisational aspects

The monitoring body must have adequate human and technical resources to perform its monitoring activities. The adequacy of the resources depends on the number, size and complexity of the code members, the type, scope and extent of their activity as determined by the code of conduct and the risk content of the processing operations covered by the code of conduct.

The monitoring body must have a sufficient number of persons (in-house personnel or external service providers) and ensure adequate remuneration for its employees.

The monitoring body is responsible for the monitoring activity and therefore shall have the appropriate decision-making powers. 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.
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.

2.2.4 Independence of the monitoring body with respect to the accountability

The monitoring body must be able to demonstrate “accountability” with respect to its decisions and actions in order to be considered to be independent. Evidence of such can be demonstrated by the definition of the tasks, the decision-making framework and adequate documentation of the procedural organisation, e.g. including appropriate role structures and reporting.

2.3 Expertise

Regardless of an internal or external monitoring body, the monitoring body must comply with Article 41 para. 2 letter a GDPR at all times in terms of availability of personnel with the expertise required in the following areas and demonstrate these to the satisfaction of the competent supervisory authority at all times:

1. Appropriate knowledge and experience in the field of data protection legislation;
2. In-depth knowledge with regard to the subject matter of the code of conduct, the processing operations covered by them and the processes in this area;
3. Technical and organisational expertise, in particular knowledge of technical-organisational measures in the area of data protection;
4. Expertise in risk assessment, in particular with respect to the rights and freedoms of data subjects;
5. Experience in the field of monitoring codes of conduct/compliance standards, including monitoring in the form of audits.

The specific requirements for the essential expertise depend on the number, size and complexity of the code members, the type, scope and extent of their activities determined by the code of conduct and the risk content of the processing operations covered by the code of conduct.

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

Personnel responsible for the management of the monitoring body must have a professional qualification and relevant professional experience in legal and technical matters), whereby legal and technical expertise may not necessarily be present in one person. In general, evidence may be provided by an EQF2[1] Level 6[2] qualification and at least five years' relevant professional experience in legal and technical matters or by an EQF2, Level 7[3] qualification and relevant professional experience of at least three years.

In addition, the monitoring body must demonstrate the existence of suitable processes for obtaining the abovementioned qualifications and experience. The expertise of the staff must be kept up to date. Evidence of this knowledge may be provided through training certificates, relevant work experience (e.g. audits conducted) or otherwise to the satisfaction of the competent supervisory authority in the accreditation process and in the ongoing monitoring, and demonstrated at the request of the competent supervisory authority.

[1] EQF2 – European Qualifications Framework

[2] Level 6 – first cycle of studies (Bachelor's degree or similar qualifications in accordance with the European Qualifications Network), with advanced expertise in an area of work or study that demonstrates a command of the subject and ability to innovate, and that solves complex and unpredictable problems in a specialised area of work or study, based on a critical understanding of theories and principles.

[3] Level 7 – second cycle of studies (Master's degree or similar qualifications in accordance with the European Qualifications Network), with highly specialised knowledge, specific abilities to solve problems as a basis for innovative thinking to gain new knowledge and to develop new procedures and to integrate knowledge from different areas.

2.4 Conflicts of interest

In accordance with Article 41 para. 2 lit. d GDPR, the monitoring body shall demonstrate that any conflicts of interest in the performance of its functions are excluded at all times. Structures must be created to avoid conflicts of interest depending on the number, size and complexity of the code members, the type, area and extent of their activities determined by the code of conduct and the risk content of the processing operations covered by the code of conduct.

To avoid conflicts of interest, the monitoring body must, in particular, be free of external (direct or indirect) influence. For example, as stated in no. 2.2, it must be able to act without instruction and be protected from measures and sanctions by the code owner and the code members through the performance of their tasks.

The monitoring body shall have a process for avoiding and managing conflicts of interest. Employees of the monitoring body shall report in writing any potential conflicts of interest or threats to independence.

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.

Neither the monitoring body nor the personnel assigned to monitoring may act beyond the actual monitoring activities of the code members or provide any other services, in particular advice on data protection issues, unless the monitoring body can demonstrate it has taken reasonable precautions to minimise any potential risk of conflict of interest. The same applies, should the monitoring body or its staff be involved in the creation of monitoring rules. For example, reasonable precautions may consist in a structural-organisational separation of these tasks from the area responsible for monitoring (e.g. Chinese Walls, see also no. 2.2.1 on internal monitoring bodies).

2.5 Outsourcing

As a matter of principle, 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, according to which

1. The requirements and obligations for the monitoring body are fulfilled in the same way by the external service provider;
2. The monitoring body maintains the same competence and experience to ensure effective monitoring of the services provided by the contracting entity;
3. Outsourcing does not result in a delegation of responsibility for the monitoring and, in any event, the monitoring body remains responsible to the 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 that fulfils the following minimum requirements:

1. The monitoring body shall have a legally binding, enforceable, written agreement with each provider of outsourced services, which contains provisions, in particular with respect to:
    a. Specification and potential delimitation of the service provided by the contractor;
    b. Expertise and independence of the personnel employed by the contractor, and assurance of impartiality, confidentiality and no conflicts of interest;
    c. Obligation of the contractor to inform the monitoring body of developments that could compromise the correct performance of the outsourced activities and processes.
2. The monitoring body shall adequately manage the risks associated with the outsourcing and monitor the execution of the outsourced activities and processes effectively.
3. 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.

2.6 Procedures and structures established by the monitoring body

2.6.1 Monitoring of the code of conduct

In accordance with Article 41 para. 2 lit. b GDPR the monitoring body must demonstrate that it has documented procedures that enable it to fulfil the following tasks and duties at all times:

2.6.1.1 Creation of the requirements prior to the start of the monitoring activities

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 and to allow for verification by the competent supervisory authorities. In particular, it shall specify the applicable standards of assessment, the principles of the verification and evaluation procedure and the key elements for the planning of the monitoring activity. The standardisation of procedures and requirements must be clarified and implemented in the verification and evaluation procedure. In addition, they shall develop appropriate procedures for updating and reviewing their own evaluation methods with respect to changes in the legal framework, relevant risks, the state of the art or amended costs of technical and organisational measures and procedures for notifying the code members of any legal or factual changes relating to the code of conduct (e.g. legislative changes, current decisions of the executive or judiciary, new state-of-the-art, etc.).

2.6.1.2 Process of the assessment of the code member

The monitoring bodies shall assess whether the code member is able to implement the code of conduct.

2.6.1.3 Verification of the application and monitoring of compliance with the code of conduct

The monitoring body must verify the application and compliance of the code members. The inspections are carried out based on a rotation principle. The required metric must be indicated. 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. A representative random sample must be taken. 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 could include random or unannounced audits, annual inspections, regular reporting and the use of questionnaires. The verification procedure could take place (additionally) on site.

In addition to the routine monitoring during the rotation tests, event-related checks may be conducted and, based on requirements defined by the monitoring body, i.e. possible main points of complaint, are essentially necessary. In particular, event-related checks may also be carried out unannounced on the code members.

2.6.1.4 Verification of suitability of the code of conduct

The monitoring bodies 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. 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.

2.6.1.5 Additional tasks

With regard to the design of the relevant code of conduct, additional tasks may arise for the monitoring bodies arising from the respective code of conduct. But these additional tasks must not affect the monitoring body's ability to carry out its tasks as a monitoring body, in particular not to impair the effectiveness and impartiality of it´s monitoring activities.

2.6.2 Documentation of the monitoring activity

In accordance with Art. 41 para. 2 lit. b GDPR the monitoring body must demonstrate that it is able to document its monitoring activities at all times and in the usual way and submit such documentation to the competent supervisory authority upon request. In addition, the application shall specify the procedures to ensure that the competent supervisory authority has an overview of the procedures in force at the time of termination of the monitoring activity and shall be presented with the relevant information on the status and content of the proceedings.

Appropriate documentation includes information regarding the inspection schedule and the evaluation process. In addition, information regarding the rules and procedures that enable

it to perform its tasks must be documented. Technical and organisational measures shall ensure the correct storage of the documentation.

The monitoring body shall maintain a directory regarding the code members to enable the code member to be identified and to indicate the validity of the respective membership, unless this is carried out by the code owner. In this event, the monitoring body must be able to access such directory.

The monitoring body shall provide its contact details to the code members, where appropriate, through the code owner.

The documentation also includes the results of the inspections and a summary statement of compliance with respect to the code member.

2.6.3 Event-related obligation to take appropriate measures with respect to companies

The monitoring body must demonstrate that it has documented procedures and structures that enable it to take appropriate action against the code member to remedy the breach and avoid future violations.

Appropriate measures shall be taken based on an objective assessment of the circumstances and in accordance with the principle of proportionality. Appropriate measures may be, for example: training measures, informing the senior management of the code member, a formal request to implement certain measures within a given reasonable time period, a temporary or permanent exclusion of the code members from the code of conduct.

2.6.4 Routine regular obligation to provide information with respect to the supervisory authorities without delay

In accordance with Article 41 para. 4 GDPR, the monitoring body must inform the competent supervisory authority in writing, at regular intervals and at least once a year, regarding the measures taken, the reasons for such and the complaint procedure. This can be in the form of a summary.

2.6.5 Event-related immediate obligation to provide information with respect to the respective code members, existing associations and supervisory authorities as a matter of urgency

The monitoring body must demonstrate that it has documented procedures and structures that enable it to promptly notify the competent supervisory authority of any serious action, i.e. suspension or expulsion from the code of conduct. Moreover, in these cases, the monitoring body must also notify the competent supervisory authority responsible for the code member in the event of cross-border code of conduct within the meaning of Article 40 para. 7 GDPR.

The monitoring body must also demonstrate that it has documented procedures and structures that enable it to promptly notify the competent supervisory authority in writing of any changes that could materially affect the monitoring activities of the monitoring body. It must be noted here that a material impairment generally exists if the amendment ceases to guarantee or jeopardises fulfilment of the requirements in accordance with no. 2.

2.6.6 Confidentiality

The monitoring body must demonstrate that it has documented procedures that enable it to maintain appropriate confidentially at all times. 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 at all times, unless the monitoring body is required to disclose such by law or is authorised to do so under the contract. The code member must always be notified prior to disclosure and given the opportunity to comment. However, the monitoring body is entitled to disclose all confidential information to the competent supervisory authority, as long as the disclosure is necessary to carry out its supervisory activities.

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

3 Powers

The monitoring body shall demonstrate that it has documented processes and structures which enable it to use the powers granted to fulfil its tasks effectively at all times in accordance with Article 40, 41 GDPR. Knowledge of the contact details and contact persons of the code members, including the responsible manager and the powers of investigation and powers to act are required to perform the tasks effectively. The relationship between the monitoring body and the code members, including the inspection of the associated competences of the monitoring body, e.g. rights to information or investigation rights, is subject to regulation by private law agreement. The regulation may be internal or external to the code of conduct, but must be binding and enforceable. However, this shall not affect the requirement that the core elements of the monitoring body´s function under the terms of Art. 40, 41 GDPR will be included in the code of conduct itself. Additional clauses may be added in the form of an agreement or contract between the monitoring body and the code member, as long as they do not entail a variation in the essential elements of the monitoring body's function, as set out in the code.

3.1 Knowledge of the contact details and contact persons of the code member, and the responsible managing director

The monitoring body shall ensure that it has the full contact details of the code members. This includes, besides the code member´s address, telephone number and email address, the contact person details. If a data protection officer is appointed for the code member, this person can also act as a contact person for the monitoring body. The monitoring body should also have information on the substitute of the contact as required (in particular during absence owing to leave or illness). Notwithstanding the above the monitoring body should in any case have the contact details of at least one member of the executive board of each code member.

3.2 Powers of investigation

Every monitoring body must implement measures to perform its task to monitor compliance with the code of conduct. The monitoring bodies must explain to the competent supervisory authority and demonstrate that the investigative powers can be used effectively with respect to the code members. Code members must ensure that the monitoring body is able to check

that the processors of the code members comply with the code of conduct. In certain cases, this can be carried out using evidence provided by the code member. For this purpose, code members must be legally bound by a regulation either inside or outside the code of conduct.

3.3 Competence to act

Every monitoring body must be able to effectively regulate any violations of the code members against their obligations in accordance with the code of conduct.

4 Complaint procedure

In accordance with Article 41 para. 2 lit. c GDPR, the monitoring body must demonstrate that it has documented procedures and structures to enable it to receive, assess and handle complaints regarding violations of the code of conduct or the way in which the code of conduct of code members are applied, and to make decisions on complaints within a reasonable time period. The monitoring body must also prove that the complaint procedure is independent, effective and transparent, and that any decisions regarding complaints have been taken in accordance with the principle of proportionality.

4.1 Documentation of proof of an appropriate complaint procedure

The complaint procedure must contain at least the following elements and procedures:

1. Procedure for the receipt (e.g. in writing, online, via email or fax, etc.), validation and investigation of the complaint, and the decision regarding the actions to take in response to such;
2. The monitoring and recording of complaints, including measures to resolve such, or the grounds for refusing to treat as a complaint;
3. Assurance that the appropriate action is taken with a reasonable period of time;
4. Notification to the complainant of the outcome of the proceedings, insofar as the complainant him/herself is involved. If the complaint procedure has not been resolved within three months from issuing of the acknowledgment of receipt, the complainant shall be notified of the progress of such.

Upon receiving a complaint, the monitoring body must verify that the complaint relates to potential violations of the code of conduct for which it is accredited as a monitoring body and, if so, process the complaint in a timely manner.

The monitoring body is responsible for collecting and verifying all the necessary information to validate the complaint. The information required is that which enables objective and non-discriminatory verification of the facts raised in the complaint.

4.2 Documentation of proof of a transparent complaint procedure

The description of the complaint procedure must be published in a form that is generally accessible following a successful accreditation of the monitoring body. Publication shall be carried out by the monitoring body. ‘Generally accessible’ is information regarding the complaint procedure, if it is clearly and easily visible, e.g. publication on the homepage of the monitoring body.

Annex 1: List of abbreviations / Glossary

The following definitions apply, unless the context indicates otherwise:

Application phase	Period between the submission of the application for accreditation with the supervisory authority responsible for accreditation and the issuing of the accreditation.
Code member	Controller or processor who committed to apply the code of conduct for which the monitoring body is seeking accreditation under Article 41 para. 1 GDPR.
Code owner	The association or other body within the meaning of Article 40 para. 2 GDPR, that has drafted, amended or supplemented the code of conduct.
Competent supervisory authority	The supervisory authority responsible for accreditation under Article 55 GDPR.