Ordinance of the Data Protection Authority on the requirements for a body monitoring the compliance of Codes of Conduct (Überwachungsstellenakkreditierungs-Verordnung – ÜStAkk-V)

[…]:

General Provisions

§ 1. This ordinance regulates the requirements for the accreditation of bodies permitted to monitor compliance with code of conduct pursuant to Art. 40 GDPR (monitoring bodies) by implementing the provisions of Article 41(2) of Regulation (EU) 2016/679 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, hereinafter "GDPR"), OJ L 119 of 4.5.2016 p. 1, as amended by the Corrigendum OJ No. L 127 of 23.5.2018 p. 2.

Accreditation Requirements and Procedures

§ 2. (1) The accreditation as a monitoring body shall not depend on any particular legal form of the applicant. The application may also be submitted by an organisational unit within those associations and other bodies, which have drafted, amended or extended the code of conduct in accordance with Art. 40 (2) GDPR (internal monitoring body).

(2) The accreditation as a monitoring body shall be based on a written application to the data protection
authority.

(3) The application shall contain proof of fulfilment of the requirements pursuant to §§ 3 to 7 as well as the following information:

1. To establish the identity of the applicant:
a) the name of the applicant or, in case of companies entered in the company register (Firmenbuch), the company name (Firma) […], as well as the company register number (Firmenbuchnummer), in case of associations the Central Register of Associations number (ZVR number) […] and if an activity in accordance with the Business and Trade Code of 1994 (Gewerbeordnung 1994 - GewO 1994, […] is performed, the Austrian Business Licence Information System number (GISA number) […],

b) in case of a legal person or a registered partnership, the name or names of the persons authorised to represent the company externally,

c) the professional title, where the applicant is entitled to use such a title,

2. the intended field or fields of activity covered by the code of conduct to be monitored, by references to and definition of the associations and other bodies that represent the categories of controllers or processors for which accreditation is sought, and,

3. for the proof of good reputation: If reliability and a clean criminal record are not mandatory for the exercise of the professional activity, a criminal record certificate or, in the case of associations, a register extract for associations according to § 89m of the Court Organization Act (Gerichtsorganisationsgesetz - GOG, […]),

4. a registered office or residence in the European Economic Area in accordance with the EEA Agreement,
and

5. to ensure the continued performance of the tasks and powers associated with accreditation: presentation
of the financial, personnel and organisational resources.

(4) The information referred to in (2) shall be accompanied by the submission of relevant documents and certificates, unless these are available from publicly accessible registers.

(5) If the application for accreditation is not submitted in the language of the supervisory authority, the information pursuant to (3) shall be provided and demonstrated by relevant documents or certificates in a verified translation.

Independence and Expertise

§ 3. (1) The applicant shall provide evidence as to the independence and expertise of the persons authorised to take decisions within the monitoring body by submitting relevant documents and certificates
in accordance with the following provisions.

(2) A monitoring body is considered independent if it has not legal, economic, financial, organisational, personal or professional dependence or relationship with the entity to be monitored, which
could question its independence and integrity regarding its activities as monitoring body.

(3) The independence shall be demonstrated by:

1. disclosure of the beneficial owners, in particular by submitting an excerpt from the register of beneficial owners kept at the registry authority pursuant to the [Act transposing Art. 30 and 31 of Directive (EU) 2015/849 and transposing Art. 1 of Directive (EU) 2016/2258],

2. information on persons authorised to make decisions, which shows that there are no personal ties with the entities to be monitored,

3. for clubs and associations by submitting its statutes,

4. information on the funding of the monitoring body.

(4) The expertise shall be demonstrated by:

1. the successful completion of a relevant course of study at an Austrian university or a foreign university or a technical college recognised as equivalent, the successful completion of a college or a relevant higher vocational school, including special types of schools, which provides the basic knowledge required for the fulfilment of the tasks, or

2. a relevant activity in the field of the code of conduct to be monitored or in the fields relevant to the organisation or sector for which accreditation is sought, and in any case

3. an excellent knowledge of data protection law and its application, including technical and organisational measures and procedures as well as sector-specific knowledge.

(5) With regard to relevant activity pursuant to (4) no. 2, it shall be permissible to include an equivalent experience in an enterprise with a different subject area.

(6) Where an application is submitted for an internal monitoring body, in addition to the provisions of (3) and (4), an organisational structure must be demonstrated for this internal monitoring body by submitting appropriate documents enabling it to fulfil its tasks with financial and organisational independence and without external influence by the association or other bodies.

Measures to prevent conflicts of interest

§ 4. (1) A monitoring body shall have appropriate measures and mechanisms in place to ensure that its tasks and obligations will not result in a conflict of interest.

(2) The qualification must be proven by a catalogue of measures - declared binding for all employees of the monitoring body -, which must in any case provide for the following:

1. Provisions on incompatibility, which stipulate that persons authorised to make decisions at the monitoring body shall not engage in any further business activity incompatible with the performance of their duties,

2. implementation of substitute rules in the event of conflicts of interest,

3. confidentiality clauses or non-disclosure agreements, and

4. freedom of instructions from those to be monitored and - if the application for accreditation is submitted for an internal monitoring body - from the association or other bodies.

Assessment and Monitoring Procedure

§ 5. (1) A monitoring body shall establish procedures to monitor the compliance with the code of conduct and to periodically review the application of the code of conduct. It should be ensured that the controllers or processors that apply the code of conduct belong to the appropriate category or field of activity.

(2) A procedure is appropriate if the audit standards specify how the audit or evaluation process should
be carried out in practice, the criteria according to which the monitoring activity should be planned and the
procedure should be evaluated on an ongoing basis. In any case, the monitoring body shall lay down basic
provisions in the audit standards on the following topics:

1. Audits, which provide for systematic investigations to be carried out in accordance with established rules, in accordance with the following procedures and criteria:

a) Schedules providing for audits to be carried out at predetermined intervals. The frequency of periodic audits shall be based in particular on the number of those to be monitored who have undertaken to comply with the code of conduct, the geographical scope, sectoral or sector-specific requirements and the number of complaints,

b) Determination of the methods to be applied and the criteria to be evaluated according to an evaluation grid.

2. Procedural guidelines enabling the monitoring body to investigate any breaches of the code of conduct, to make findings and, where appropriate, to take appropriate measures as laid down in the code of conduct.

(3) The appropriateness of the procedure pursuant to (2) shall be demonstrated by a conceptual description of the monitoring procedure.

Dispute Settlement Procedure

§ 6. (1) In accordance with the following provisions, the monitoring body shall establish guidelines for a complaint procedure with regard to infringements of the code of conduct or the application of code of conduct by controllers or processor, whereas it shall provide evidence of the relevant procedures and structures by submitting adequate documents.

(2) The procedural guidelines shall ensure that disputes are assessed within a reasonable time, in a simple and transparent manner and on the basis of an objective assessment of the circumstances and with due regard to the rights of the parties.

(3) The procedural guidelines shall specify in particular:

1. details of the persons responsible for dealing with complaints, including their appointment and intended period of service,

2. in the case of an establishment of a collegial decision-making body, the right of the parties to appoint a natural person to that body,

3. the right of the parties to comment on statements of the opposite party within a reasonable period of time, which should be determined by the monitoring body,

4. an obligation to notify in such a way that the complainant is to be informed within three months of the progress of the proceedings,

5. reasons that can prevent the treatment of a complaint, and

(4) After successful accreditation, the procedural guidelines shall be published in a generally accessible manner.

(5) The monitoring body shall keep a record of the complaints it has received and the actions it has taken and shall give the data protection authority access to it at any time.

Actions taken by the Monitoring Body

§ 7. (1) In the event of infringements of the code of conduct by a controller or a processor, the monitoring body shall establish - and proof their existence by submitting relevant documents and certificates - procedures to take appropriate actions to remedy infringements and to prevent repeated offences.

(2) The following actions can be foreseen:

1. the imposition of restrictions, combined with a threat of exclusion from the code of conduct if compliance with the restrictions is not proven,

2. instructions or guidance that facilitate compliance,

3. the assessment of non-compliant behaviour, combined with a determination of the cause and proposals of remedies to remove the cause, as well as

4. temporary or, in the case of repetition or serious infringements, the final exclusion from the code of conduct.

(3) The controller or processor shall be notified in writing of the action taken and the reasons for it.

(4) An action pursuant to (2) may be waived if the controller or processor has taken appropriate measures and the infringement has been rectified.

Reporting obligation

§ 8. (1) The monitoring body shall submit to the data protection authority a report on the activities carried out during the previous year until 31 March of every year. The reporting obligation under Art. 41(4) last sentence GDPR remains unaffected. In any case, the data protection authority must be informed immediately of any serious measures, such as provisional or definitive exclusion from the code of conduct.

(2) The monitoring body shall establish internal reporting mechanisms providing for regular reporting to the data protection authority, in particular on the results of monitoring procedures pursuant to § 5.

(3) Irrespective of the annual reporting obligation pursuant to (1), the data protection authority shall be notified of any circumstance or significant change that no longer enables the monitoring body to perform its duties.

Procedure for reviewing the code of conduct

§ 9. (1) The monitoring body shall provide for appropriate procedures enabling it to review the code of conduct to determine whether they require amendment.

(2) A procedure shall be considered appropriate if it is based on the results of the procedures pursuant to section 5 (2), the number of complaint procedures and the grounds for the complaint as well as the measures taken in the event of infringements of the code of conduct.

[…]