Detailed version (with examples) of the accreditation requirements for code of conduct monitoring bodies

General remarks:

Article 40.4 of the GDPR provides that codes of conduct shall contain mechanisms enabling the body referred to in Article 41 of the Regulation to monitor compliance with said codes. Such bodies may be internal or external (as *ad hoc* committees). The requirements listed below shall apply to the monitoring body, whether internal or external.

"The supervisory authority" referred to in the requirements below is the French data protection authority (hereinafter the CNIL).

Requirements	Examples of supporting documents
1. General requirements	
Explanatory note: These requirements aim to set out a general framework for the monitoring body's activities. They also include the guarantees that it must provide to demonstrate proper management of its activities and its financial and material independence.	
1.1 The monitoring body shall implement an approach aiming to ensure that all processing operations it performs for its monitoring tasks are compliant with the GDPR.	For instance, that approach can be materialized through : - a record of processing activities - a data management policy
1.2 The monitoring body shall demonstrate that all appropriate human, financial and material resources in proportion with the code of conduct's scope are used. Such resources are adapted to the number and size of code members and to the level of complexity or risk of the processing carried out by code members.	A document explaining the allocation of human and material resources for its monitoring tasks. When an internal body is appointed: a description of functions and an organisational chart. Certificate of insurance (professional liability) covering its monitoring tasks. Any other evidence of financial assets.

Requirements	Examples of supporting documents
1.3 The monitoring body's obligations and the core elements of its function are set out in the code of conduct.	Additional clauses may be added in the form of an agreement or contract between the monitoring body and the code member, provided that it does not result in a change to the key elements of the monitoring body's function.
1.4 The monitoring body shall ensure that the documents relating to the performance of its duties (documents provided, audit plan, audit evidence, audit reports, etc.) are stored in a way that maintains their confidentiality or are definitely and securely destroyed if they are no longer of when the monitoring tasks are over (subject to other legal obligations or legitimate grounds).	Examples: - Non-disclosure agreement template - Service agreement template - Procedure to destroy or archive documents (for documents that must be archived as a legal requirement). - Procedure protecting the confidentiality of documents (management of user profiles, management of identifiers, etc.)
1.5 The monitoring body shall ensure when performing its tasks; that it complies with the security measures provided by the code member. These security measures shall not prevent the monitoring body from performing its tasks.	Security measures refer to the appropriate technical and organisational measures implemented by the code member (as data controller or data processor) to ensure and be able to demonstrate that processing is carried out in compliance with the GDPR (pursuant to Article 24 of the GDPR). Example: the monitoring body ensures that it requests communication of anonymised documents or the submission of standard templates.
2. Requirements relating to the monitoring body's independence	
Explanatory note: A monitoring body's independence is ensured by implementing formal rules and procedures which govern its appointment, its mandate and its functioning. When requesting accreditation from the supervisory authority, the monitoring body must demonstrate its functional, material and decision-making independence. Compliance with each requirement will be assessed in light of the supporting documents provided.	

Requirements	Examples of supporting documents
The requirements and examples listed below shall apply to the monitoring body, whether internal or external.	
2.1 The monitoring body shall demonstrate its independence, particularly with regards to the code owner, the code members and members of the specific sector of the code.	For external monitoring bodies: a code of ethics or any other document demonstrating the body's independence. For internal monitoring bodies: any relevant (contractual or organisational) document demonstrating its independence.
2.2 The monitoring body shall demonstrate its functional independence with regards to the code owner and code members when performing its tasks and exercising its powers. The monitoring body must have the necessary human and technical resources to efficiently perform its tasks. The monitoring body shall demonstrate that it is able to fully perform its monitoring duties, taking into consideration the specific sector and the risks associated with the processing activities to which the code of conduct applies.	These organisational aspects may be proven by the recruiting process of the personnel within the monitoring body, the remuneration of said personnel, as well as the duration of missions, contracts or any other formal agreement between the personnel and the monitoring body.
2.3 The monitoring body shall demonstrate its financial independence by providing evidence of sufficient financial resources and financial viability to perform its duties. The monitoring body shall demonstrate that the rules relating to its financing prevent any risk of compromising its independence or the performance of its tasks, including from a code member.	Example: specific budget allocated to the internal monitoring body.
2.4 The monitoring body shall demonstrate its independence during the decision-making process, including the choice of its personnel entrusted with monitoring duties.	Any relevant (contractual or organisational) document may be provided.

Requirements	Examples of supporting documents
2.5 The monitoring body shall demonstrate that it is solely responsible for decision-making when performing its monitoring tasks. Without prejudice to the supervisory authority's tasks and powers, decisions made by the monitoring body relating to its functions are not submitted to another body for approval; including to the code owner.	Example: Documents or procedures clearly setting out the respective roles of each, the functioning of the decision-making process and reporting procedures. The documentation provided may also include job descriptions, management reports and policies aiming to raise personnel awareness of governance structures and procedures in place.
3. Requirements relating to the absence of conflicts of interest	
Explanatory note: The absence of conflicts of interest is ensured by implementing measures and procedures aiming to prevent such situations.	
3.1 The monitoring body shall remain free from any direct or indirect external influence. It shall not seek nor take instructions from any person, organisation or association.	Internal monitoring bodies must be protected against any form of sanction or (direct or indirect) interference from the owner of the code, bodies representing categories of data controllers or processors, or code members, as a result of the performance of its tasks.
3.2 The monitoring body shall be able to identify any situation likely to create a conflict of interest (due to its personnel, its organisation, its procedures, its subcontractors, etc.)	Any relevant document. Examples: - Specific internal procedure - questionnaire to be completed by the personnel and the subcontractor - Templates of forms enabling the personnel, including the subcontractor's personnel, to report a conflict of interest

Requirements	Examples of supporting documents
3.3 The monitoring body shall implement procedures and measures to avoid conflicts of interest so as to refrain from any action incompatible with its duties and functions. The monitoring body must set out a procedure to handle any situation likely to create a conflict of interest.	Examples: Standard clauses enabling personnel, including the subcontractor's personnel, to opt-out from a task due to a conflict of interest.
3.4 The monitoring body must have its own personnel, selected by itself or by a service provider that is independent from the code.	Example: - an independent service provider may be a third party with specific expertise on the subject of the code This may be demonstrated by providing evidence. The documentation provided may pertain to recruitment procedures, job descriptions, etc.
4. Requirements relating to the monitoring body's expertise	
Explanatory note: Each request for accreditation is assessed in concreto, also taking into account the specific expertise requirements set out by the code of conduct. Expertise requirements are set out taking into account various factors such as the specific sector of the code of conduct, the size of this sector, the number of code members, the risks tied to the processing activities and the different interests at stake.	
4.1 Requirements relating to management personnel in charge of the decision-making process	
4.1.1 The monitoring body shall demonstrate that it has the necessary expertise to properly perform the monitoring activities under the code of conduct.	The monitoring body sets out the rules to assess its management personnel's knowledge and skills. These criteria may be changed if

Requirements	Examples of supporting documents
	it appears that they do not enable the monitoring body to properly perform its duties.
4.1.2 The monitoring body shall demonstrate that the personnel in charge of the decision-making has in-depth knowledge on and experience in the topics and issues relating to data protection and in the specific sector the code of conduct addresses, as well as in the performance of monitoring tasks. Such expertise is not necessarily concentrated by one single individual.	In any case, this level of knowledge and experience in the legal and technical field is higher than the one expected from the audit personnel.
4.2 Requirements relating to personnel performing monitoring tasks	
4.2.1 The personnel shall have undergone training on audit methods (audit principles, audit procedures and techniques, documents relating to audits, regulations and other applicable requirements, etc.).	Provide evidence of a recruitment process taking into account auditors' training in audit methodology. Provide evidence of an internal training. Job description template.
4.2.2 The personnel shall have taken part in at least two full audits, from their preparation to the final conclusions, in the last three years.	Template of a signed statement.
4.2.3 The personnel shall be able to benefit from continuing training.	Personnel continuing training programme (technical, legal or audit).
4.2.4 The personnel shall have the necessary level of expertise as regards the processing activities referred to in the code and in-depth knowledge on the data protection topics relating to the specific sector of the code.	The monitoring body will demonstrate and provide evidence of a recruitment process taking into account these specific knowledge and experience.

Requirements	Examples of supporting documents
4.2.5 The personnel shall have undergone a specific training on personal data protection.	Provide evidence of a recruitment process taking into account their training (specific degree or certification in data protection law).
4.2.6 The personnel with a legal profile shall hold a minima a first year Master's degree or an equivalent degree in the legal field.	Job description template. Provide evidence of a hiring or assignment process including this requirement.
4.2.7 The personnel with a legal profile shall have at least two years of professional experience in the field of personal data protection (e.g. consulting, litigation, etc.).	Job description template. Provide evidence of a hiring or assignment process including this requirement.
4.2.8 The personnel with a technical profile shall hold *a minima* a bachelor's degree or an equivalent degree in the field of computer sciences, information systems or cybersecurity.	Provide evidence of a recruitment or assignment process taking account of such training.
4.2.9 The personnel with a technical profile have undergone at least a two days' training on relevant standards for information system security management (regulations, standards, methods, best practices, risk management, etc.).	Provide evidence of a recruitment or assignment process taking account of such training.
4.2.10 The personnel with a technical profile shall have at least two years' experience in the field of information system security.	Provide evidence of a recruitment or assignment process taking account of this requirement. Provision of a standard job description indicating required skills.
5. Requirements relating to the monitoring body's procedures	
Explanatory note:	

Requirements	Examples of supporting documents
These requirements aim to guarantee that the monitoring tasks and duties carried out by the monitoring body are regular, complete and transparent for the member of the code of conduct. The monitoring procedure can be shaped in different ways such as random or unannounced audits, annual inspections, regular reporting and the use of questionnaires. The monitoring procedure implemented by the monitoring body is in accordance with the framework given by the code of conduct.	
5.1 The monitoring body must demonstrate that the audit procedure sets out which expertise is necessary to perform its tasks and guarantees that the personnel possesses the necessary expertise to conduct the monitoring tasks.	Produce any document justifying the implemented measures to meet this requirement. E.g., a standard framework note explaining the skills required to perform the monitoring tasks.
5.2 The monitoring body shall demonstrate that the monitoring procedure includes a commitment from the personnel to comply with the rules pertaining to ethics, independence, unbiased presentation of results and the use of a methodical approach.	Template of statement of principles that each member of personnel has to fill in.
5.3 The monitoring body shall demonstrate that the procedure provides for regular controls, carried out in an independent manner and which enable: – an assessment of data controllers' and/or processors' eligibility to adhere to the code of conduct; – a monitoring of the compliance with the code after adherence, and – a review of the proper functioning of the code's operation	Produce any document proving the implementation of such a procedure.

Requirements	Examples of supporting documents
5.4 The monitoring body shall demonstrate that it has put in place a monitoring programme which takes into account such elements as the complexity of processing operations and the risks associated with the data processing, the number of code members, the code's geographic scope and the received complaints.	Provide the monitoring programme used by the monitoring body to monitor code members. E.g.: - Prioritize code members audits based on the large number of complaints sent to the monitoring body or the processing of sensitive data. - Audit code members by rotation
5.5 The monitoring body shall demonstrate that the monitoring procedure ensures the integrity and traceability of evidence when collecting necessary information.	Complete audit report template (including reports, observations, comments made by the code member, etc.)
5.6 The monitoring body shall demonstrate that the monitoring results and conclusions are presented and explained to audited code members within a reasonable period of time. In the context of a monitoring, written or oral comments made by a code member upon receipt of findings and conclusions are listed in the report.	The reasonable period of time shall be set out in the code of conduct. Template of a report drafted after collection of relevant evidence.

6. Requirements relating to the processing of complaints
Explanatory note: The monitoring body implements procedures to ensure the impartial and objective processing of complaints pertaining to code violations or the manner in which the code is applied by a code member. These procedures are transparent and public to all.

The handling complaint procedure established by the monitoring body handles complaints from a code member or from any person who can demonstrate a legitimate interest. This process should be sufficiently resourced and personnel should demonstrate sufficient knowledge and impartiality. This procedure is also based on the applicable code of conduct.	
6.1 The monitoring body shall establish a procedure to receive, manage and process complaints. The monitoring body shall demonstrate that this procedure is unbiased and transparent.	Template of complaints handling procedure (including contact details, how the complaint is presented, how the complaint is followed-up on, etc.) This procedure specifies, for example: - how the complainant is informed - the consequences should the complaint be rejected - the consequences should the complaint be considered justified.
6.2 This procedure shall be accessible and easily understood by all, including data subjects and code members.	Standard contact form and/or screenshot of monitoring body website.
6.3 The monitoring body ensures that all complaints are processed and provides the complainant with reports on the procedure's progress or its results within a reasonable period of time, e.g. three months, as from receipt of the complaint. The period required for resolution of the complaint may be extended for a reasonable period where necessary, taking account of the complexity of the complaint. The monitoring body shall inform the complainant of such an extension within three months as from receipt of the complaint and specify the reasons for extending the deadline.	Template of acknowledgment of receipt of complaints, response template, etc. Every decision must be justified.

6.4 The monitoring body shall keep a record of the processing of all complaints received. The monitoring body keeps this record readily available to the supervisory authority, which may access it at any time.	Template of sheet recording complaints received and processed. This record includes the nature of the complaint, the identity of the concerned code member and of the complainant, the forms and delays of complaints handling and the reason for closing the complaint.
6.5 The monitoring body shall make its decisions, or general information thereof, publicly available, pursuant to its complaints handling procedure. Such general information may include, but is not limited to, general statistical data on the number and type of complaints/infringements received and the resolutions/corrective measures issued. Such general information must include information relating to the sanctions having resulted in the suspension or exclusion of a code member.	

7. Requirements relating to information of the supervisory authority	
Explanatory note: These requirements list the information that a monitory body must provide to the supervisory authority on a regular basis.	
7.1 The monitoring body shall compile in a single document the summaries of all of the actions undertaken. The document is at the disposal of the supervisory authority which can access it at any time.	In particular, this document contains code revision reports, the measures taken against code members, etc.
7.2 The monitoring body shall inform the supervisory authority, without undue delay and in writing, of any substantial change	

(particularly relating to structure or organisation) likely to call into question its independence, expertise and the absence of any conflict of interests.	
7.3 The monitoring body shall inform the supervisory authority, in writing, when a binding measure is taken against a code member. This notice includes the reasons justifying the measure. The frequency of communication is based on several criteria, including the seriousness of the infringement and of the adopted measure.	Any relevant document proving the measures implemented to meet this requirement. Example: procedure to inform the CNIL.
7.4 The monitoring body shall inform the supervisory authority, without undue delay and in writing, as soon as a code member is suspended. This notice includes the reasons justifying the measure.	Any relevant document proving the measures implemented to meet this requirement. Example: procedure to inform the CNIL.
7.5 The monitoring body shall inform the supervisory authority, without undue delay and in writing, as soon as a code member is excluded from the code of conduct. This notice includes the reasons justifying the measure.	Any relevant document proving the measures implemented to meet this requirement. Example: procedure to inform the CNIL.
8. Requirements relating to review mechanisms	
Explanatory note: The code owner may decide to change or extend the code's scope and/or its content. In that case, monitoring bodies are involved in this process: they play a key role by contributing to the update of the code of conduct pursuant to the review mechanisms set out by the code of conduct.	

8.1 The monitoring body participates in the review and/or changes to the code decided by the code owner.	
8.2 The monitoring body must set out procedures to implement and monitor the application of the changes decided by the code owner.	
8.3 The monitoring body also provides the code owner with a periodical report on the proper functioning of the code's operation.	
9. Requirements relating to legal status	
9.1 Requirements relating to the monitoring body	
9.1.1 The monitoring body is established in the European Union.	Example: provision of a Kbis certificate
9.1.2 The monitoring body remains responsible to the supervisory authority, for all tasks and decisions relating to its duties.	
9.1.3 The monitoring body has sufficient financial, human and material resources and has procedures ensuring the continuity of its monitoring duties for the duration of its accreditation.	
9.2 Requirements relating to the management of subcontracting	
Explanatory note:	

The aim of these requirements is to ensure compliance with this accreditation requirements when the monitoring body subcontracts parts of its tasks.	
9.2.1 The monitoring body shall establish a contract or any other legal act under European Union law binding on the subcontractor with regard to the monitoring body in such a way that all subcontracted tasks will meet the requirements of the GDPR. Recourse to subcontracting does not result in the delegation of responsibilities: in any case, the monitoring body remains responsible for monitoring compliance with the code of conduct to the supervisory authority.	Subcontracting agreement template
9.2.2 The monitoring body ensures that all subcontractors meet the requirements set out by this accreditation requirements document, notably as regards independence, absence of conflict of interest and expertise.	Any relevant document attesting to the subcontractor's independence, expertise and absence of conflict of interest in relation to its tasks.
9.2.3 The monitoring body includes a specific clause in the contract signed with subcontractors to ensure the confidentiality of personal data that may, where applicable, be disclosed to the subcontractor during the monitoring tasks.	Template of non-disclosure clause
10. Requirements relating to the sanctions and corrective measures decided by the monitoring body	
10.1 The monitoring body applies the corrective measures and sanctions set out in the code of conduct.	The code of conduct includes a matrix of corrective measures which must be applied by the monitoring body. These corrective measures are applicable in cases of violations of the code by a member. The sanctions include, for example, suspension or exclusion of the concerned data controller or processer from the code.

10.2 When it enforces the application of corrective measures or issues sanctions in accordance with the code of conduct, the monitoring body shall ensure that the code member's rights are respected.	Any document attesting to the implementation of measures to meet this requirement. Example: - Dispute resolution procedure indicating the adherent's rights - notice template indicating the code member's rights