Opinion of the Board (Art. 64)

Opinion 12/2024 on the draft decision of the French Supervisory Authority regarding the “Code of Conduct for Service Providers in Clinical Research” submitted by EUCROF

Adopted on 18 June 2024

Table of contents

The European Data Protection Board

Having regard to Article 63, Article 64(1)(b) and Article 40 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 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 (hereinafter "GDPR"),

Having regard to the European Economic Area (hereinafter "EEA") Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) Member States, Supervisory Authorities, the European Data Protection Board and the European Commission shall encourage the drawing up of codes of conduct (hereinafter "code") to contribute to the proper application of the GDPR[2].

(2) The main role of the European Data Protection Board (hereinafter "the EDPB") is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter "SA") intends to approve a code of conduct that related to processing activities in several Member States (hereinafter "transnational code") pursuant to Article 40.7 GDPR and to the Board's "Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679" (hereinafter the "Guidelines").

(3) The EDPB welcomes and acknowledges the efforts made by the associations and others bodies representing categories of controllers or processors to elaborate codes of conduct which are practical and potentially cost-effective tools to ensure greater consistency among a sector and foster the right to privacy and data protection of data subjects by increasing transparency.

(4) This opinion aims to ensure the consistent application of the GDPR, including by the SAs, controllers and processors and to highlight the core elements which each code of conduct has to develop.

(5) Taking into account the specific characteristics of the sector concerned, each code of conduct should be addressed individually and is without prejudice of the assessment of any other code of conduct. The EDPB recalls that Codes represent an opportunity to establish a set of rules which contribute to the proper application of the GDPR in a practical, transparent and potentially cost-effective manner that takes on board the specificities for a particular sector and/or its processing activities.

(6) The EDPB underlines that codes of conduct are voluntary accountability tools, and that the adherence to a code does not prevent SAs from exercising their enforcement power and prerogatives.

[1] References to "Member States" made throughout this opinion should be understood as references to "EEA Member States".
[2] Article 40(1) GDPR

(7) The present code is not a code of conduct according to Article 46(2)(e) meant for international transfers of personal data and therefore does not provide appropriate safeguards within the framework of transfers of personal data to third countries or international organisations under the terms referred to in point (e) of Article 46 (2). Indeed, any transfer of personal data to a third country or to an international organisation shall take place only if the provisions of chapter V of the GDPR are respected.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in the guidelines on codes of conduct[3], the EUCROF draft Code of Conduct for Service Providers in Clinical Research ("EUCROF draft code", "draft code" or "code") was reviewed by the French Supervisory Authority as the Competent Supervisory Authority (hereinafter the "CompSA").
2. The EUCROF Code has been reviewed according to the procedures set up by the EDPB.
3. The CompSA has submitted its draft decision regarding the draft EUCROF Code, requesting an opinion of the EDPB pursuant to Article 64(1)(b) GDPR on 5 February 2024. The decision on the completeness of the file was taken on 12 March 2024.
4. In compliance with Article 10(2) of the Board Rules of Procedure, due to the complexity of the matter at hand, the Chair decided to extend the initial adoption of eight weeks by further six weeks.

2 ASSESSMENT

2.1 General remarks

5. The Board welcomes the references to the EDPB Opinion in footnote 1 on "the explanation of the distinction between consent obtained for clinical research participation and consent for processing of personal data", the EDPB Guidelines in footnote 13 on "the territorial scope of GDPR (Article 3)", the EDPB Guidelines in footnote 14 on "personal data breach notification under the GDPR". However, the Board notes that the references to the EDPB are missing, thus it recommends the FR SA to require the code owner to add this reference to the relevant footnotes, for clarity purposes.

2.2 On the Code of conduct meeting the needs of the sector

[3] Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/676 adopted by the EDPB on 4 June 2019.

2.2.1 Presentation of the sector

6. Clinical research corresponds to scientific studies carried out on the human person, with a view to the development of biological or medical knowledge. There are two types of Clinical Studies: interventional studies (also called clinical trials) and observational studies.

7. Clinical research projects are usually initiated by a sponsor (e.g. a pharmaceutical company). For the implementation of these studies, the sponsor may use the services of a contract research organisation ("CRO"). Contracts between clinical research projects' sponsors and CROs specify the services to be provided and they contain the CRO's obligations pursuant to Article 28 GDPR.

8. The Board notes that the draft code refers to pharmaceutical laboratories instead of companies. There Board encourages the FR SA to require the code owner to replace this term with the term "companies" for accuracy purposes.

9. The EUCROF draft code covers both clinical trials and non-interventional research. The purpose of the code is to describe the obligations of the service providers in clinical research, as processors within the meaning of Article 28 GDPR, in the context of the performance of the contract between them and the sponsor.

2.2.2 The code owner as a representative organisation

10. Codes of conduct must be submitted for approval to the supervisory authority which is competent in accordance with Article 55 GDPR. In case of transnational codes, when identifying the competent SA, some factors could be taken into account, for example, the location of the largest density of the processing activity or the location of the code owner's headquarters[4].

11. The code owner is the European Contract Research Organization ("CRO") Federation "EUCROF" which is a not-for-profit legal entity registered in the Netherlands. In section 1.1 of the Code, the code owner explains that their objectives are "among others, to contribute to Clinical Research in humans and to promote the excellence of European Clinical Research to the public and the media, as well as on the international stage". The members of EUCROF are national CRO associations as well as individual CROs established in one or more European countries or outside Europe, as defined in its Bylaws. To date, according to the Code, EUCROF has more than 360 affiliated companies in 25 countries, and over 300 of these affiliates are SMEs.

12. The code owner has identified the French supervisory authority as the competent supervisory authority for the purposes of seeking approval of the EUCROF Code. The code owner has justified his choice in the code of conduct based on the competent supervisory authority's "proximity to the location of a large density of the CROs in Europe", and the fact that the French supervisory authority "has considerable experience in the protection of Personal Data in the field of healthcare and Clinical Research, having undertaken initiatives to publish tools and guidelines to assist organisations and companies with GDPR compliance"[5]. The Code also emphasized that the choice of the competent authority "is without prejudice of the powers

[4] See Appendix 2 to the Guidelines.
[5] Section 1.7 of the Code.

given to all supervisory authorities by GDPR and the supervisory authorities retain all powers granted to them under Article 55 of the GDPR"[6].

13. In accordance with Article 40 (2) GDPR, a code of conduct has to be prepared by associations or others bodies representing categories of controllers or processors (code owners). Because the code owner plays a major role in ensuring consistency and harmonization of practices within the sector concerned by the code, it has to demonstrate to the CompSA that it is an effective representative organization. As such, as stated in the Guidelines, the code owner should be capable of understanding the needs of their members and define the processing activity or sector to which the code is intended to apply[7].

14. Recital 99 GDPR advises to consult during the process of drawing up a Code of Conduct with relevant stakeholders. Section 1.1 of the Code states that the task force in charge of drafting the code "has widely consulted the EUCROF affiliates, as well as representatives of other stakeholders: pharmaceutical industry, patient associations, medical devices companies, representatives of ethics committees, representatives of various academic organisations, lawyers specialized in electronic health systems as well as experts in ISO certifications". The EDPB notes that code owner has demonstrated that it is an effective representative body, capable of understanding the needs of their members.

2.2.3 Processing Scope

15. Clinical research projects are initiated by a sponsor (e.g. a pharmaceutical company). For the implementation of these studies, the sponsor may use the services of a contract research organisation ("CRO"). Contracts between clinical research projects' sponsors and CROs specify the services to be provided and they contain the CRO's obligations pursuant to Article 28 GDPR.

16. The draft code covers both clinical trials and non-interventional research. The purpose of the code is to describe the obligations of the service providers in clinical research, as processors within the meaning of Article 28 GDPR, in the context of the performance of the contract between them and the sponsor.

17. The Board welcomes the detailed explanation of this draft code of conduct's scope in section 1.8. In this section it is mentioned that "a legal entity acting as sub-processor for another legal entity of the same group of companies acting as the Sponsor of a Clinical Research (data controller) is eligible for adherence to this code of conduct". It is not clear for the Board why the term sub-processor is used in this section. Therefore, the Board encourages the FR SA to require the code owner to clarify this in the code or replace this term with the term "processor".

18. Furthermore, with respect to section 1.9.2 of the draft code on the "exclusion from this code of conduct", the Board notes that "This Code of Conduct does not intend to cover exhaustively all contractual patterns that may occur between a Sponsor and a CRO and there is no such an obligation for a Code of Conduct to cover all industry activities in the GDPR". Regarding this part of the code and what is excluded from this code's scope, the Board encourages the FR SA to require the code owner to more clearly state what is not covered by this code by adding further examples of what is excluded from the code.

[6] Section 1.7 of the Code.
[7] See para. 22 of the Guidelines.

19. Section 1.8 of the draft code describes that it aims at covering all data processing activities associated with the services that the adhering CROs deliver to sponsors in the context of service contracts and where CROs are acting as processors and the sponsors as controllers.

20. Appendix 2 of the draft Code ("Classes of services in scope of this Code") encloses a list of the most common types of processing activities covered by the Code, including their purpose, the types of personal data processed, and the duration of the processing. The Board highlights that the duration of the processing is to be decided by the controller. Therefore the Board recommends the FR SA to require the code owner to include a general comment so to clarify that the information provided under "duration of the processing" in the code for all the services, is to be determined by the data controller.

21. Processing activities "carried out by both Sponsors and CROs that fall outside this contractual relationship", and "processing activities performed by the CRO as a data controller in its own right" are excluded from the scope of the Code[8].

2.2.4 Territorial scope

22. The scope of the EUCROF draft code is transnational and is intended to apply across the European Union, as per Article 40 (7) GDPR. The EUCROF draft code has identified all European Union supervisory authorities as concerned SAs. The EDPB notes that the scope of the code does not cover EEA States.

23. The Board notes that Appendix 1 of the draft code lists the concerned SAs. The Board encourages the FR SA to require the code owner to check the accuracy of the names and contact details of the SAs.

24. For instance, the list does not reflect the federal structure of the independent German SAs. As CROs as well as sponsors in Germany (e.g. private companies, universities or hospitals) are usually under the jurisdiction of the state SAs, they should also be mentioned and a reference (e.g. link) should be added. A full list of German state SAs ("Datenschutzaufsichtsbehörden der Länder") can be found here: https://www.datenschutzkonferenz-online.de/datenschutzaufsichtsbehoerden.html

2.3 On the code of conduct facilitating the effective application of the GDPR

25. The Guidelines state that Codes will need to specify the practical application of the GDPR and accurately reflect the nature of the processing activity or sector. They should be able to provide clear industry specific improvements in terms of compliance with data protection law. A code shall not just re-state the GDPR. Instead, it should aim to codify how compliance with the GDPR can be achieved in a specific, practical and precise manner[9]. Furthermore, the code has to provide sufficient appropriate safeguards to mitigate the risk around data processing and the right and freedoms of individuals[10].

26. The EUCROF draft code contains both strict requirements particularizing the provisions of the GDPR mentioned in the "Processing Scope" section of the present Opinion and good practices

[8] Section 1.8 of the Code.
[9] Para. 36-37 of the Guidelines.
[10] Para. 39 of the Guidelines.

currently followed by the sector. The EUCROF draft code helps CROs to understand clearly what their obligations are under the GDPR, facilitates best practice compliance by CROs and improves upon the state of the art for data protection in the sector[11]. In addition, it helps sponsors to optimise and simplify the process to monitor compliance of adhering CROs with the GDPR[12].

2.3.1 The code as a practical tool

27. The EUCROF draft code brings clarity as to what GDPR requirements mean in practice when applied by CROs, and what are the actual measures which CROs will take to ensure compliance with the GDPR. The EUCROF draft code describes the rights and obligations of adhering CROs on the basis of key GDPR principles such as purpose limitation, data subject rights, transfers, security, auditing, liability, etc.

2.3.2 Matrix of requirements

28. The draft Code consists of a set of requirements that CROs have to implement to comply with the Code.

2.3.3 Binding nature of the Code

29. All provisions of the draft code and EUCROF security objectives and requirements are binding for the classes of services defined in the Statement of Applicability by the CRO for which the adherent CRO declares compliance with the Code. Throughout the Code, the provisions make use of “shall” and “must”. Some provisions should be regarded as guidance, setting examples of good practices and are denoted by the use of the terms “should” or “may”.

2.3.4 On the Code provided safeguards

30. In line with the Guidelines[13], a code of conduct must provide sufficient safeguards while being adequately focused on particular data protection areas and issues in the specific sector to which it applies (“added value”). The EUCROF draft Code provides sufficient safeguards by, for instance, adopting the same terminology as the one used in the GDPR (Code, section 1.4) and providing complaint mechanism to data subjects (Code, section 5.7). In terms of added value, the draft code provides guidance adapted to the sector on, among others, security measures, auditing requirements, data subject rights and transparency requirement.

31. The Board takes note of the section 2.2.1 of the draft code, where it is mentioned that “Except if otherwise instructed by the Sponsor and required by the delivered services / processes, CROs shall not process data that identify the Study Subject directly. Study Subjects shall only be identified with a Study specific subject identification code, which constitutes pseudonymisation per Article 4(5) of the GDPR”. The Board is of the opinion that this provision of the code is not sufficient and recommends the FR SA to require the code owner to specify the aim (needs) of the pseudonymisation process and better determine the circumstances and the safeguards

[11] Section 1.6 of the Code.
[12] Section 1.6 of the Code.
[13] See para. 36 of the Guidelines.

under which CRO's may exceptionally have access to the identity of study subject if necessary either in section 2.2.1 or in section 3.6.3 of the draft code.

32. Similarly, the Board recommends the FR SA to require the code owner to add references to EDPB guidance and recommendations on pseudonymisation methods.

33. Similarly in section 3.6.1 of the draft code of conduct on "pseudonymisation" under the note the code states "CRO should ensure that the codes are robust enough as a method of pseudonymisation and present a random sequence of symbols with no easily recognisable pattern within one Study that might pose a re-identification risk". The Board notes that the reference to "no easily recognisable pattern" is not enough and recommends the FR SA to require the code owner to delete the term "easily", but also to further clarify that CRO takes into account the risk of identification and chooses the appropriate techniques to mitigate the risk identified.

34. The Board notes that the draft code under section 3.2.2 of on the secondary use of personal data for scientific research purposes, refers to the legal basis for such processing mentioning "Article 5(1)(b) and Article 6(1) and (4) GDPR". The Board recommends the FR SA to require the code owner to clarify in the code that Articles 5(1)(b) and 6(4) GDPR do not necessarily apply cumulatively, where the further processing operations pursue scientific research purposes. In addition, the code should also refer to Article 9(2) GDPR when the processing concerns special categories of personal data for scientific research purposes. Therefore, the Board recommends the FR SA to require the code owner to modify section 3.2.2 accordingly.

35. The Board notes that service class 17 (i.e. provision of physical hosting infrastructure) is excluded from section 3.6 on "integrity and confidentiality" of the draft code. The Board is of the opinion that the requirements of section 3.6 shall also apply to service class 17, thus recommends the FR SA to require the code owner to modify this provision of the code accordingly.

36. Regarding section 3.4.2.1 of the draft code "on data collection by healthcare professionals" with respect to the following (under section 3.4.2.d) reference "Note that in some cases, e.g., DICOM image data sets, automatic "anonymisation" processes may be implemented at the time of upload into the eCRF", the Board recommends the FR SA to require the code owner to replace the term "anonymisation" with the term "pseudonymisation", since it understands that this is going to be the case.

37. Similarly, in the same section of the draft code and in order to avoid ambiguity, the Board recommends the FR SA to require the code owner to clarify whether the term "may be" refers to the use of the automatic tools for the pseudonymisation of images.

38. In section 3.5.f the draft code mentions that "The CRO shall delete or anonymise any data for which it cannot identify a specified necessity or purpose. Data destruction or anonymisation shall be performed in accordance with recognised industry standards and shall be verified to ensure that all Personal Data has been removed or securely overwritten". According to Article 28(3)(g) GDPR it is not up to the processor (CRO) to decide whether they should anonymise personal data or delete them after the agreed service ends. Pursuant to Article 28(3)(g) GDPR, personal data must be deleted or returned and existing copies must be deleted unless Union or Member State law requires the storage of personal data. In the same section of the draft code on page 34, the third example outlines a situation where the sponsor orders the CRO to save personal data for the sponsor, e.g. for secondary use, therefore this processing would fall

under the service contract. The measure 3.5.f only concerns data for which a purpose cannot be identified within the service contract. Therefore and in order to ensure consistency with the GDPR, the Board recommends the FR SA to require the code owner to delete the reference to the anonymisation of the data, to align the wording of this provision of the code with Article 28(3)(g) GDPR, and to clarify that the CRO will act upon controller's instructions.

39. Moreover, section 4.2 of the draft code of conduct on "Technical and organisational measures" mainly focuses on the establishing and maintaining of an Information Security Management System ("ISMS"), referring to the ISO 27001 standard. Section 4.2 also refers to ISO 27701 (Extension to ISO 27001 for privacy information management), the code document 02 (matrix & requirements) lists 12 ISO 27701 requirements. According to Article 32 GDPR technical and organisational measures include further requirements than an ISMS. An ISMS could indeed be an integral part of the GDPR technical and organisational measures, but the goals of an ISMS and Article 32 GDPR differ considerably. When selecting suitable technical and organisational measures, Article 32 GDPR takes the perspective of the data subjects and their exercise of fundamental rights and therefore differs from the perspective of IT Security. ISMS focuses on information security and is intended to protect the data processing institution and thus is not enough to ensure compliance with Article 32 GDPR. Considering the above, the Board recommends the FR SA to require the code owner to clarify in the code that referring to ISMS is not enough to ensure compliance with Article 32 GDPR.

2.3.5 The Code as an accountability tool

40. The objectives of the EUCROF draft code are the following[14]:

- Define the requirements of the GDPR, taking into account the national and international Clinical Research regulations applicable to the data processing activities of CROs in force from time to time[15], and imposing these requirements to the adhering CROs;
- Propose a clear compliance model for both small and large CROs and thus assist CROs to be compliant with GDPR rules by providing them with a set of good practices and operating methods suitable for the Clinical Research industry;
- Optimise and simplify the process for a Sponsor to monitor compliance of adhering CROs with the GDPR;
- Establish trust by improving the transparency of processing of Personal Data in Clinical Research to stakeholders (Sponsors, Study Subjects, regulatory bodies, Investigators, and the other members of the Clinical Research team);
- Establish a common and acknowledged base for the security of information systems for Clinical Research used and/or provided by CROs, and thus favour and facilitate innovation, adoption, and proper use of new technologies within Clinical Research[16];
- It has to be noted that a harmonised approach on the security of information systems, based on already acknowledged standards, does not mean that there is a harmonisation of the positions of the EU member states regarding the adoption of

[14] Section 1.6 of the Code.
[15] The code shall be revised if new substantial recommendations or guidelines are published, depending on their impact on any specificities of the Code. However, the generalities of the code are considered to be sufficient enough that a CRO can be compliant with new guidelines without a code revision.
[16] Examples of the central connection between data protection and innovation in clinical research can be seen in the EMA Recommendation paper on decentralised elements in clinical trials of 14 December 2022.

innovation in specific application areas (e.g., eCRF, eConsent, eSource, rSDV, eTMF, IoT and connected objects for real life studies etc…);

- Provide a clear governance model at European level, that has received a favourable opinion from the European Data Protection Board and the approval from the competent supervisory authority.
- Such governance model has legal effect for the organisations who adhere to the Code and for those that rely upon CROs' adherence to said Code, as the Code can be used as an element by which to demonstrate compliance with the requirements set out within the GDPR; and
- Assist the harmonisation of GDPR implementation in Clinical Research by all stakeholders and throughout the European Union.

41. The Board recommends the FR SA to require the code owner to add in Appendix 3 and 4, in addition to the Chair of the Supervisory Committee ("COSUP"), the Vice Chair for completeness purposes to cover all roles in COSUP.

2.4 On the mechanisms for monitoring compliance with a code

42. As per Article 40(4) GDPR and the Guidelines[17], a code requires the implementation of suitable mechanisms to ensure that its rules are appropriately monitored and that efficient and meaningful enforcement measures are put in place to ensure full compliance. A code specifically needs to identify and propose structures and procedures which provide for effective monitoring and enforcement of infringements.

2.4.1 Adherence to the Code

43. The code has to detail an adhesion mechanism.

44. An effective adhesion mechanism has to develop a process divided on three phases which coincide with the code of conduct "lifetime". During the first phase, the mechanism must precise that the code members must comply with all the Code requirements and that the monitoring body will assess the eligibility of candidate to the code. In a second phase, the mechanism shall describe how that monitoring is carried out on an ongoing basis and in a third phase on ad hoc basis[18]. The EUCROF Code develops an adhesion mechanism which fulfills the three phases of monitoring.

45. With respect to section 5.5.6 of the draft code on "level 2: third party assessment", para. 5, the Board encourages the FR SA to require the code owner to add, in addition to the "approval, or conditional approval" the possibility of rejection.

46. The draft code provides for two adherences mechanisms: 1. CRO's declarative process period of the documentation provided by the applicant (the level 1 "declarative adherence procedure" described in section 5.5.5 of the Code) and 2. a monitoring adherence period an on-site audit (the level 2 "third party assessment" described in section 5.5.6). In both cases, the monitoring body ("COSUP") validates the membership. Decisions of the COSUP to declare a CRO as adhering to the code have a period of validity of 3 years starting from the date of the decision. In addition, adherent CROs must comply with all provisions of the Code (for the services) regardless of whether candidate CRO is applying for level 1 or level 2. The Board believes, with

[17] See para. 40 of the Guidelines.
[18] Para. 70 of the Guidelines.

respect to the first adherence mechanism, that a mere a check list by the candidate wanting to adhere to code, should not be enough to meet the requirements for adherence. In particular, the candidates CROs shall provide detailed documentation proving their compliance with all the provisions of the code. Furthermore, it shall be made clear in the code that the monitoring body has the power to request the candidate CRO to provide additional documents if needed. The Board recommends the FR SA to require the code owner to take all the above into account and modify the relevant provisions of the code accordingly.

2.4.2 The monitoring of the Code

47. The Board notes that in section 5.1.2 on Legal Responsibility and Liability the draft code states that "EUCROF has legal responsibility with regard to the monitoring of this Code of Conduct, and will assume full liability for any breaches of the COSUP's obligations under Article 41(4) GDPR. EUCROF has all insurances and reserves to cover the risks inherent to these operations". The Board, firstly, notes that this provision is not consistent with the FR SA's accreditation requirements for monitoring bodies (section 9.1.2), where it is mentioned that "the monitoring body remains responsible to the supervisory authority, for all tasks and decisions relating to its duties", since in the relevant provision of the code the entire legal liability falls on the code owner (EUCROF) and not on the monitoring body (COSUP). Therefore, the Board recommends the FR SA so to require the code owner that this section is amended and brought in line with the FR SA's accreditation requirements for monitoring bodies.

48. Moreover, the Board notes that the monitoring body (COSUP) is an internal monitoring body, which is not a legal entity and that there is no possibility for a sanction towards COSUP. The Board recommends the FR SA to require the code owner to provide that the monitoring body remains responsible to the supervisory authority, for all tasks and decisions relating to its duties and that the code owner takes the necessary steps to ensure this.

    The Board notes that under section 5.2.2 of the draft code, "[t]he Chairman and Vice-Chairman of the COSUP shall be elected by and from among the Members of the COSUP. Subject to the initial installation process described in section 5.2.6, they shall be selected by means of a simple majority vote by all Members of the COSUP". The Board also understands that, under the rules set by the draft code, in a given mandate, the elected Chairman and Vice-Chairman of the COSUP could potentially both be CROs' representatives. In order to better represent the diversity of COSUP members and to avoid CROs to be over-represented, the Board recommends the FR SA to require the code owner to provide that, in a given mandate, the Chairman and Vice-Chairman cannot both be CROs' representatives at the same time.

49. Finally, the EDPB recalls that the code of conduct will not be operational before the designated monitoring body is accredited[19].

2.4.3 Sanctions

50. In accordance with article 40 (4) GDPR and the Guidelines, without prejudice to the tasks and powers of the competent supervisory authority, the monitoring body designated by the code owner shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor. Those sanctions range from non-public but formal

[19] Where several monitoring bodies are designated by the code, the accreditation of one of them is sufficient to provide to the code of conduct a binding nature.

reprimand to temporary or permanent revocation from the Code. The monitoring body commits to inform the competent supervisory authority about any related actions taken (Code, section 5.8).

51. To ensure transparency to code members, the code shall include a list of corrective measures which must be applied by the monitoring body. For this purpose, the EUCROF Code develops an enforcement framework which determines the appropriate sanction to be followed by the monitoring body.

2.4.4 The review of the code

52. As per Article 40 (2) GDPR and the Guidelines, the code sets out an appropriate review mechanism to ensure that the code remains relevant to legal and technical standards. In particular, section 5.10 of the EUCROF Code provides that a regular review of the Code to reflect legal, technological or operational changes and best practices shall take place when appropriate.

3 CONCLUSIONS / RECOMMENDATIONS

53. By way of conclusion, the EDPB:

1. recommends the FR SA to require the code owner to add the reference to the EDPB to the relevant footnotes;
2. recommends the FR SA to require the code owner to specify the aim (needs) of the pseudonymisation process and better determine the circumstances and the safeguards under which CRO's may exceptionally have access to the identity of study subject if necessary either in section 2.2.1 or in section 3.6.3 of the draft code;
3. similarly, recommends the FR SA to require the code owner to add references to EDPB guidance and recommendations on pseudonymisation methods;
4. in section 3.6.1 of the draft code of conduct, recommends the FR SA to require the code owner to delete the term "easily" but also to further clarify that CRO takes into account the risk of identification and the appropriate techniques to mitigate the risk identified;
5. recommends, with regards to section 3.2.2, the FR SA to require the code owner to clarify in the code that Articles 5(1)(b) and 6(4) GDPR do not necessarily apply cumulatively, where the further processing operations pursue scientific research purposes. In addition, the code should also refer to Article 9(2) GDPR when the processing concerns special categories of personal data for scientific research purposes.
6. regarding service class 17, recommends the FR SA to require the code owner to modify the code so that the requirements of section 3.6 apply;
7. in section 3.4.2.d, recommends the FR SA to require the code owner to replace the term "anonymisation" with the term "pseudonymisation";
8. in the same section, recommends the FR SA to require the code owner to clarify whether the term "may be" refers to the use of the automatic tools for the pseudonymisation of images;

9. in section 3.5.f, recommends the FR SA to require the code owner to delete the reference to the anonymisation of the data, to align the wording of this provision of the code with Article 28(3)(g) GDPR, and to clarify that the CRO will act upon controller's instructions;

10. in section 4.2, recommends the FR SA to require the code owner to clarify in the code that referring to ISMS is not enough to ensure compliance with Article 32 GDPR;

11. in appendix 2, recommends the FR SA to require the code owner to have a general comment so to clarify that the information provided under "duration of the processing", for all the services, is to be determined by the data controller;

12. in Appendix 3 and 4, recommends the FR SA to require the code owner to add the Vice Chair in addition to the Chair of the Supervisory Committee (COSUP);

13. regarding the adherence mechanism, recommends the FR SA to require the code owner to amend the relevant provisions of the code so that candidate CROs to level one provide detailed documentation proving their compliance with all the provisions of the code of conduct, and the monitoring body has the power to request the candidate CRO to provide additional documents;

14. regarding the monitoring of the code, recommends the FR SA to require the code owner to amend section 5.1.2 so that it is in line with the provisions of the FR SA's accreditation requirements for monitoring bodies, which states that "the monitoring body remains responsible to the supervisory authority, for all tasks and decisions relating to its duties";

15. similarly, recommends the FR SA to require the code owner to provide that the monitoring body remains responsible to the supervisory authority, for all tasks and decisions relating to its duties and that the code owner takes the necessary steps to ensure this;

16. in section 5.2.2, recommends the FR SA to require the code owner to provide that, in a given mandate, the Chairman and Vice-Chairman cannot both be CROs' representatives at the same time.

54. Finally, the EDPB also recalls the provisions of Article 40 (5) GDPR and that in case of amendment or extension of the EUCROF Code of conduct, the CompSA will have to submit the modified version to the EDPB in accordance with the procedures outlined in the Guidelines approved by the EDPB.

4 FINAL REMARKS

55. This opinion is addressed to the FR SA and will be made public pursuant to Article 64(5)(b) GDPR.

56. According to Article 64(7) and (8) GDPR, the FR SA shall communicate its response to this opinion to the Chair by electronic mean within two weeks after receiving the opinion, whether it will amend or maintain its draft decision. Within the same period, it shall provide the amended draft decision or where it does not intend to follow the Opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this Opinion, in whole or in part.

57. Pursuant to Article 70(1)(y) GDPR, the FR SA shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

58. As per Article 40(8) GDPR, the Board shall submit this opinion to the European Commission.

For the European Data Protection Board
The Chair

(Anu Talus)