General Data Protection Regulation

GDPR

Code of Conduct

For

Service Providers in Clinical Research

Presentation Note

08 March 2021

EUCROF, p/a GroenHoed, Pelmolenlaan 2, 3447 GW WOERDEN, The Netherlands – VAT Number: NL8172.84.369.B01
www.eucrof.eu | info@eucrof.eu

1 Foreword, rationale

Articles 40 of Regulation 2016/679 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, also known as "GDPR", "*[…] encourages drawing up of code of conducts intended to contribute to the proper implementation of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.*"

In addition, article 41 specifies that "*[…] the monitoring of compliance with a code of conduct pursuant to article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter […].*"

During the last quarter of year 2017, EUCROF's New Technology Working Group, analyzing the impacts of this forthcoming regulation on clinical research activities throughout Europe, acknowledged:

a) Pursuant to article 40 GDPR, Clinical research is a field with highly specific features, where a number of specific Regulations apply, and the vast majority (over 90%) of Service Providers for Clinical Research, also known as "CROs" – Contract Research Organizations" are micro, small and medium-sized enterprises;

b) All stakeholders, including the largest CRO organizations that are regional or global players, favor higher harmonization across the European Members States;

c) Pursuant to article 41 GDPR, EUCROF, as a European corporate non-profit organization, has the required expertise in relation to the subject-matter;

d) The need for continuous improvement of quality, security and confidentiality management, to foster transparency and create trust, in a technology driven domain with many new players and growing involvement of patients;

e) CROs mainly act a Processors with regard to Data Protection and article 82 "Right to compensation and liability" recital 2 of GDPR specifies "*[…] A processor shall be liable for the damage caused by processing only where […] it has acted outside or contrary to lawful instructions of the controller*", creates a new area of responsibility that needs to be well delineated and managed.

In its General Assembly meeting held in Madrid in November 2017, EUCROF members voted for the elaboration of a code of conduct applying to CROs, and:

- Mandated the New Technology Working Group to establish an International Task Force for the elaboration of this Code and engage all required consultations with stakeholders and regulatory bodies;
- Voted a budgetary line to support this specific and strategic activity;

This task force has now accomplished its first mission and delivered the so-called EUCROF Code of conduct also referred to as "EUCROF Code" or the "Code" in this document.

This Code is now being introduced in the formal approval process as defined in the Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 of the European Data Protection Board (EDPB).

The purpose of this document is to provide an overview of the Code: who is the owner, how the Code has been designed to adapt to the high heterogeneity of CROs and effectively fulfill the evidenced gaps, what kind of governance etc…

2 About the European CRO Federation

The EUCROF is a not-for-profit legal entity registered in the Netherlands whose objectives are:

1. To contribute to a high quality of Clinical Research in humans, by improving the knowledge, competence/expertise and skills related to Clinical Research of its Members, by:
   a. Exchanging relevant information between Members;
   b. Developing training and educational programmes for Clinical Research. Supporting the Members in setting up these educational programmes and safeguarding the quality of these programmes;
2. To represent and promote the position of its Members, whose activities are geared towards providing services related to Clinical Research in humans, by:
   a. Forming a legal entity to represent and support the interests of its Members towards regulatory authorities, the pharmaceutical, biotech, medical device, and other healthcare-related industries within the field of Clinical Research, as well as patients and the medical and affiliated research community;
   b. Developing and maintaining a close relationship and mutual understanding among Members, patients and affiliated professional groups, regulatory authorities, pharmaceutical industry, biotech industry, medical device industry, healthcare-related industry within the field of Clinical Research and other international organisations within the area of Clinical Research;
   c. Distributing information on developments in Clinical Research to relevant stakeholders;
3. To promote the excellence of European Clinical Research towards the public, the media, as well as on the international scene.

The members of EUCROF are national CRO associations as well as individual CROs (with a different membership scheme) established in 25 European countries. Today EUCROF has more than 360 affiliated companies, in 25 countries. More than 300 of these companies are falling under the SME definition of the EU.

Considering its federative role, the Federation intervenes under the principle of subsidiarity whenever and wherever it is in a better position to support the interests of its Members, rather than each individual Member alone, and in the position to support the common interests of its Members, particularly at the European scale.

EUCROF decision-making is performed by the General Assembly of its members. The list of EUCROF members, as well as EUCROF bylaws, are public and can be freely downloaded from EUCROF's website (www.eucrof.eu).

Day to day management and representation of the Federation is performed by an Executive Board (EB) consisting in a group of elected executives (President, Vice-President, Secretary, Treasurer, Executive Board member). EB mandates are for 2 years.

EUCROF's financial resources come (a) first from the regular annual fees paid by its members, (b) ad'hoc complementary budget lines contributed by its members and affiliates on a voluntary basis to subsidize strategic initiatives and (c) income from the training and educational programmes and events sponsored and organized by EUCROF.

EUCROF organizes every 2 years the European Conference on Clinical Research. The 5th edition took place in Amsterdam, in February 2020 and the next edition will take place in Madrid in February 2022.

EUCROF develops its activities through working groups consisting in subject-matter experts selected among the affiliated CROs and contributing on a voluntary basis.

3 Ownership of the Code

The development of EUCROF Code has been subsidized and performed by EUCROF on its own budget and resources. Moreover, this first version of the Code addresses specifically the processes implemented by CROs for the purpose of clinical research.

Thus, EUCROF is the owner of the Code in its current release.

However, it must be noted that, future versions of the Code may extend its scope to other stakeholders and such ownership could then be transferred to an independent multi-stakeholders entity still to be created.

In the course of the elaboration of this Code and pursuant to recital 99 GDPR, representatives of numerous stakeholders (patient associations, industry, academic or European Research Infrastructure Consortia) have been consulted and such perspective has been several times envisaged and has already a pre-approval status by EUCROF decision making bodies.

4 Scope

This Code of Conduct is **a transnational code** that covers the processing activities carried out **in all the Member States of the European Union** by the CROs who adhere to this Code.

This Code covers **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.

Processing activities carried out by both Sponsors and CROs that fall outside this contractual relationship are excluded from the scope of this Code.

The types of Services in scope of the Code are listed and described in an appendix of the Code.

Because the descriptions of these "types of Services" have a generic meaning, they are referred to as "**Classes of Services**".

Such Services may concern any type of Clinical Studies, including interventional and non-interventional studies, as well as primary and secondary use of Clinical Study Data.

Personal Data considered in scope of this Code includes the Personal Data of **Study Subjects and Healthcare Professionals** processed in the frame of the Services delivered by the CROs to Sponsors.

5 Competent Supervisory Authority

The Supervisory Authority identified as the Competent Authority to manage the application procedure for submission of this Code of Conduct and act as the supervisory lead in ensuring that this Code of Conduct is being monitored effectively is the French Data Protection Authority - **CNIL (Commission Nationale de l'Informatique et des Libertés)**.

CNIL was considered as the most appropriate and suitable Authority for such role taking into account its proximity to the location of a large density of the CROs in Europe in combination with the fact that CNIL 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 in order to assist organizations and companies with GDPR compliance.

6 What exactly is a CRO ?

A Contract Research Organisation (also called Clinical Research Organisation, CRO), is a natural or legal person (including commercial, academic and non-profit) that provides services to Sponsors and other stakeholders such as governmental organisations, foundations or hospitals, on a contract basis and within the scope of Clinical Research (experimental or observational) as well as other activities in connected domains.

This definition has been created and approved by EUCROF in 2017 and has been incorporated in the last version of the Code of Conduct for Scientific Independence and Transparency in the Conduct of Pharmacoepidemiological and Pharmacovigilance Studies endorsed by the ENCeP/ EMA steering group.

This definition is inclusive of all types of "Service Providers" in the domain of Clinical Research. In particular, it includes providers of IT solutions, such as Electronic Data Capture (EDC) vendors and vendors of all types of information systems that are dedicated to Clinical Research and have to comply, or provide compliance features with, the industry specific regulations and guidance, such as FDA's 21 CFR Part 11; ICH Guidelines E6 (R2) Good Clinical Practice (GCP).

Any CRO, affiliated or not to EUCROF, can adhere to the Code.

7 CROs acting as "Processors"

The roles of Data Controller and Data Processor shall be considered in this Code of Conduct with the sole objective to define the relationship that needs to be set-up between stakeholders involved in the same Clinical Research activity regarding their respective obligations in relation with GDPR.

According to the GDPR, the Data Controller is the organisation that defines the purposes and the means of the data processing. In Clinical Research, the purpose is defined in the protocol and the means are defined (a) in the protocol, (b) the monitoring plan, (c) the data management plan and (d) the statistical analysis plan.

When considering the contractual relationship between the Sponsor and its subcontracted CROs, all of these documents are, according to ICH Guidelines E6 (R2) Good Clinical Practice (GCP), the responsibility of the Sponsor.

Therefore, this Code of Conduct addresses the most common contractual patterns where the Sponsor bears solely the role of Data Controller for the Clinical Research and the subcontracted CRO adhering to this Code is acting as a Data Processor.

8 A clear distribution of responsibilities regarding Data Protection

Pursuant to article 82 "Right to compensation and liability" recital 2 of GDPR

> *[…] A processor shall be liable for the damage caused by processing only where […] it has acted outside or contrary to lawful instructions of the controller.*

This Code is built on the requirement that the Sponsor and the CRO shall agree on a clear distribution of responsibilities regarding Data Protection and this is the purpose of the **Service Contract**.

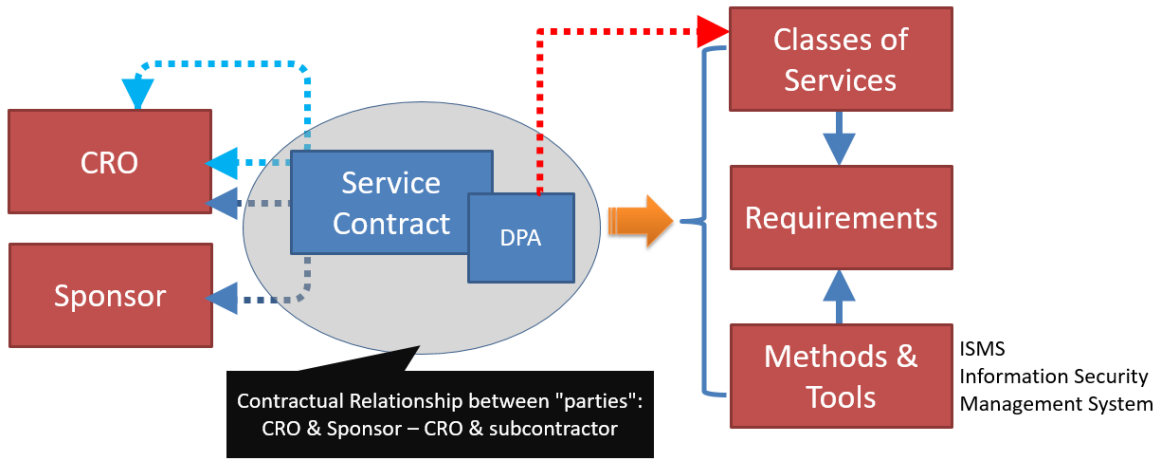
The same scheme shall apply when a CRO subcontracts with another CRO or provider for some of the services it provides to the sponsor / Controller.

The conditions concerning Data Protection laid down in the Service Contract altogether constitute the **Data Processing Agreement (DPA)** between the Parties to the Service Contract. These conditions can be included in the main Service Contract, for instance as an appendix, or in a separate contract as illustrated in the diagram below.

The conditions set in the Service Contract shall not contradict any applicable regulation and in particular GDPR.

Altogether, the Service Contract and its attached DPA, constitute the contractual relationship established between the CRO and the Sponsor that will enable to identify the respective responsibilities and liabilities of the Parties regarding Data Protection **in case of dispute or legal action**.

This Code is based on the fact that such responsibilities and liabilities directly depend on the services delivered by the CRO to the Sponsor. The Service Contract shall mandatorily define what are the services and related deliverables provided to the Sponsor by the CRO (respectively the subcontractor to the CRO).



A clear distribution of responsibilities ruled by a contractual relationship.

The "Service Contract" and the Data Processing Agreement (DPA) specifically addressing Data Protection matters.

9 A compliance scheme adapted to each company profile

Like for any "certification" process, this Code establishes a list of "**requirements**" against which "compliance" is granted and monitored.

In total, 237 requirements have been specified and listed: 84 are specific of this Code and are specified in the master document of the Code; 113 correspond to the requirements of ISO 27001 standard and 40 additional requirements address the specifics of IT managed services, including the provision of physical IT infrastructure, and are taken from different existing Standards.

CROs present multiple "company profiles", from small enterprises with a few employees delivering very specific services (i.e. data management or biostatistical analysis services only) to large, full services multinational companies. The large variety and heterogeneity of the delivered services is a specificity of the domain.

Clearly, a small CRO delivering one single service with limited impact in terms of Data Protection[1] and no dedicated online IT Platform, does not need to comply with all 237 requirements.

Compliance to this Code depends on the **CRO's profile** defined by the **Classes of Services** the CRO sells to its Clients, be them Sponsors or other CROs.

Therefore, the first requirement is specified as follows:

1.9	An adherent CRO shall define a **Statement of Applicability** listing all classes of services for which the adherent CRO declares compliance with the Code.

[1] i.e. *Synopsis, protocol and CRF design* or *Site selection and contract.*

Note that in the Code document, requirements are identified by a unique reference (in the example above "1.9") and are presented in a framed paragraph.

The **Statement of Applicability for every adherent CRO will be public** and listed on EUCROF's web site.

The Code includes a matrix mapping all Classes of Services with all the corresponding Requirements as illustrated below.

Statement of Applicability / Requirements	Class of Service 1	Class of Service 2	Class of Service 3	…	Class of Service 20
Requirement 1	Yes		Yes		
	…		…		
Requirement "n"	No		Yes		
…	…		…		

This approach enables to drop all requirements that are not applicable for the adherence of the particular CRO. It applies to all CROs falling under the definition of **small and medium enterprises** as defined by the European Commission[2].

This Code considers that large multinational and full services CROs shall comply with all 237 Requirements of the Code and shall be ISO 27001 certified. Similarly, CROs delivering IT Infrastructure or IT Managed Services shall be ISO 27001 certified.

10 All adherent CROs shall have an Information Security Management System (ISMS)

This Code takes account of the fact that the vast majority of CROs, whatever their size, already have an ISO 9001:2015 certified **Quality Management System**. They are used to the collection of the necessary corresponding records to demonstrate throughout time, the maintenance of such QMS and its continuous improvement.

This Code also makes the assumption that, depending on the Statement of Applicability, maintenance of the appropriate security and confidentiality management measures to ensure the appropriate level of Data Protection **requires** the establishment and maintenance of an **ISMS – Information Security Management System** and this ISMS can be designed as an extension of the QMS to incorporate the necessary technical and organizational security measures.

11 Documents of the Code

This Code of Conduct is made up of a set of documents. This set can only be considered in its entirety: none of these documents, taken in isolation, can be considered as constituting the Code.

Every document has a unique ID number, starting with "01" and then incremented by 1 for each additional document. Except if otherwise specified, all documents are available as PDF files.

These documents are the following:

[1] Document "01" including its appendixes, is the "master" document specifying all main features of the Code and in particular all requirements specific to Clinical Research; **Appendix 2 specifies the Classes of Services in scope of the Code**. The list of these Classes of Services is also attached hereto as annex 1.

[2] Document "02"; title "Model of Data Processing Agreement – Controller/Processor";

[3] Document "03"; title "Model of Data Processing Agreement – Processor/Sub-processor"

[2] See https://ec.europa.eu/growth/smes/sme-definition_en.

[4] Document "04"; title "Requirements Specifications & Mapping with Classes of Services". This document is available both as PDF and as XLS file.

[5] Document "05"; title "Recommendations on legal basis and information to data subjects".

[6] Document “06”; title “Delivery of supplementary patient services in a study by a CRO”.

In any of the above documents, reference to the other documents is made using the ID number and the title as listed above. The ID number is shown between brackets (ex.: [02]) in the header of every document of the Code.

12 Monitoring body

With this Code, EUCROF appoints an internal body, called Supervisory Committee (herein also referred to as COSUP) with all required capacities pursuant to article 41 GDPR "Monitoring of approved codes of conduct".

The COSUP is the body which has "*the appropriate level of expertise in relation to the subject-matter of the code and is accredited by the competent supervisory authority*".

The COSUP is the only body entitled to exercise operational decision-making regarding the adherence of CROs to the Code.

Members are physical persons with a minimum of 10 years of experience in at least one of the following domains: (1) research in the domains of health, epidemiology, genetics, biostatistics, human and social sciences, (2) protection of Personal Data, (3) health information systems, (4) the protection of the rights of patients, or (5) relevant experience of audit, inspection or certification processes.

Membership of the COSUP shall reflect a balanced representation of stakeholders interested in the Code. Thus the COSUP Members shall include at least two (2) representatives from each category below:

- Representatives of CROs. In this case, Members cannot also sit with voting powers on any of the other decision-making bodies of EUCROF: the Executive Board, the Full Members Board, the General Assembly;
- Representatives of patient associations, healthcare professionals (investigational sites), organisations producing or commercialising health products, including pharmaceutical companies, manufacturers of medical devices and biotechnology;
- Independent experts with documented experience in one or more of the above domains.

Members shall all be employed by different companies / organisations, meaning that two (2) Members of the COSUP cannot be employed by the same company / organisation.

To ensure independence, impartiality and the absence of conflicts of interests, the processes ruling the operations of the COSUP shall be compliant with ISO Standards 17065 "*Requirements for bodies certifying products, processes and services*" and 17024 "*Conformity assessment — General requirements for bodies operating certification of persons*".

Chapter 5 of document [1] details the whole organization regarding "Monitoring & Compliance". The governance is details in sub-sections 5.1 to 5.4

13 Conditions of adherence

13.1 Eligibility

Any CRO organisation delivering at least one service falling in the Classes of Service in scope of the Code is eligible and can adhere to the Code. This applies equally to EUCROF members and to non-members.

13.2 Approval of adherence

The decision to approve a Candidate CRO as adhering to the Code is the exclusive responsibility of the Supervisory Body (COSUP) and shall be subject to a formal decision through a vote of the Members of the COSUP.

13.3 Public Register

A register of adherent CROs shall be available for on-line consultation by the public in EUCROF website. This “Public Register" is the only official listing of adherent CROs. For every listed CRO, the register publishes the corresponding statement of applicability and the adherence mark.

14 Appendix 1 – Classes of Services in scope of the Code

For each Class of Service, the Code includes a general description and a table presenting an overview of the subject matter, purpose, nature, duration of the processing, and the types of personal data.

The Classes of Services in scope of the Code are the following:

(1) Synopsis, protocol and CRF design

(2) ICF design & information leaflet

(3) Site selection and contract

(4) Data Collection

(5) Monitoring

(6) Medical monitoring

(7) Pharmacovigilance (PV) and Safety Reporting

(8) Patient services

(9) Data Management

(10) Statistical Analysis

(11) Clinical Study Report (CSR)

(12) Financial Management

(13) Public Disclosure

(14) Translation of study documents/data

(15) Audits

(16) Provision of IT managed services

(17) Provision of physical hosting infrastructure

(18) User / Technical Support & Hotline

(19) Decommissioning services

(20) Maintenance of Trial Master File (TMF)

(21) Archiving Services

(22) Regulatory/Study start up Services

(23) Arrangement of Investigator Meetings

End of document