General Data Protection Regulation

GDPR

01

Code of Conduct

For

Service Providers in Clinical Research

Version 1 Draft 14

20 July 2024

EUCROF, Tappersweg 12T, 2031 ET, Haarlem, The Netherlands – VAT Number: NL8172.84.369.B01
www.eucrof.eu | treasurer@eucrof.eu

Table of contents

1 Introduction

The EUCROF GDPR Code of Conduct for Service Providers in Clinical Research (hereinafter also referred to as the "Code" or the "EUCROF Code") defines the general requirements for the engagement of contract research organisations (CROs) and other providers of specialised Clinical Research services as a data processor under the GDPR. EUCROF invites CROs of all sizes and providing all types of specialised services in the domain of clinical trials to join the Code. Once an adhering member, a CRO can declare their covered services as compliant with the Code with a Compliance Mark, and thereby is committing to rigorous data protection safeguards that are required for Clinical Research.

1.1 The European CRO Federation as the Owner of the Code of Conduct

This Code of Conduct is developed, administrated, and funded by the European CRO Federation (the EUCROF) and this is referred to as the “Code Owner”.

The EUCROF is a not-for-profit legal entity registered in the Netherlands whose objectives are, among others, to contribute to high quality 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 as defined in its bylaws. 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, EUCROF intervenes under the principle of subsidiarity whenever and wherever it is in a better position to support the interests of its members and their common interests, 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 EUCROF is performed by an Executive Board consisting of a group of elected executives (President, Vice-President, Secretary, Treasurer, Executive Board member). Executive Board 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 subsidise strategic initiatives and (c) income from the training and educational programmes and events sponsored and organized by EUCROF.

Every 2 years, EUCROF organises the European Conference on Clinical Research.

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

This Code of Conduct has been drafted by a dedicated international task force established under the umbrella of the New Technologies Working Group. This task force 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.

1.2 Documents of the Code of Conduct

The present version of the Code was developed with consideration to applicable data protection legislation and the regulations specific to the domain of Clinical Research, in force at the time of writing. This being said the Code is not intended to contain the provisions that may be established by sector specific national legislation and regulations on the protection of Personal Data of any and all countries in which the adhering CRO may be located. CROs adhering to the Code shall assist the Sponsors in determining the applicable data protection requirements with consideration to the Clinical Research-related laws.

This Code of Conduct is made up of the following two (2) documents:

- Document "01" is the present document titled "EUCROF Code of Conduct for Service Providers in Clinical Research" including its appendixes. It is the "master" document specifying all main features of the Code.

  "Notes" in this document are designed to provide a second level of reading with additional clarifications on the main plain text. Notes shall be considered with the same binding power as the plain text.

- Document "02"; titled "Security Objectives and Requirements". This document is available both as PDF and as XLS file.

These 2 documents can only be considered in conjunction: neither of these documents taken in isolation, can be considered as constituting the Code.

For more details on the structure of this Code and how the adhering CROs can achieve compliance, refer to section 1.10 hereinafter.

EUCROF has issued a number of documents that are intended as support documents. These documents **are not part of the Code** nor are they approved for use by the European Data Protection Supervisory Authorities. This “toolbox” contains templates and informational documents facilitating the implementation of the Code by the adhering candidates. The use of these tools is neither prescriptive nor mandatory. This means that CROs may use all or some of the tools at their own free choice.

Note:

Requirements of the Code are identified by a unique reference that refers to its chapter and section (for example one of the first requirements is 2.4.a) and are presented in a framed paragraph.

1.3 Glossary of terms

COSUP	Supervisory Committee of the Code
CRF	Case Report Form (see also eCRF meaning electronic Case Report Form)
CRO	Contract Research Organisation
DPA	Data Processing Agreement.
EDC	Electronic Data Capture
EDPB	European Data Protection Board
EEA	European Economic Area
EU	European Union
EUCROF	European CRO Federation
GDPR	General Data Protection Regulation
ICF	Informed Consent Form (also known as a Patient Information Sheet)[1]
PRO	Patient Reported Outcome (see also ePRO meaning electronic Patient Reported Outcome)
SME	Small & Medium Enterprise
TMF	Trial Master File (see also eTMF meaning electronic Trial Master File)

[1] See EDPB Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) for explanation of the distinction between consent obtained for clinical research participation and consent obtained for processing of Personal Data.

1.4 Terminology, Definitions

(1) Anonymous information

As per GDPR recital 26, anonymous information means information which does not relate to an identified or identifiable natural person or to Personal Data rendered anonymous in such a manner that the data subject is not or no longer identifiable. Anonymous information is not subject to the requirements of the GDPR.

(2) Applicable Regulation

In this document, applicable regulation means the GDPR and any EU national data protection laws implementing the GDPR, the EU regulations specific to the domain of clinical research, and the technological standards governing the processing of health Personal Data in computing systems.

(3) Clinical Study and Clinical Research (also just Study or Research)

A Clinical Study is a research study involving human volunteers (also called Study Subjects) that is intended to add to medical knowledge, performed under Applicable Regulation such as, in particular, Regulation No. 536/2014 on clinical trials and the Regulation No. 745/2017 on medical devices. The term Clinical Research refers to Clinical Studies in general.

There are two types of Clinical Studies: interventional studies (also called clinical trials) and observational studies.

An interventional study is a type of Clinical Study in which Study Subjects are assigned to groups that receive one or more intervention/treatment (or no intervention in the case of a control group) so that researchers can evaluate the effects of the interventions on biomedical or health-related outcomes. The assignments are determined by the study's protocol. Study Subjects may receive diagnostic, therapeutic, or other types of interventions.

An observational study is a type of Clinical Study in which Study Subjects are identified as belonging to study groups and are assessed for biomedical or health outcomes. Study Subjects may receive diagnostic, therapeutic, or other types of interventions, but the Investigator does not assign Study Subjects to a specific interventions/treatment. A patient registry is a type of observational study.

In the frame of this Code of Conduct, the term Clinical Research shall be considered in its broader meaning, including interventional and observational studies, real life studies and all types of studies with secondary use of patient data, whether collected by means of paper or electronic media, including electronic Case Report Forms (eCRFs), electronic Patient Reported Outcomes (ePROs) or electronic Clinical Outcome Assessments (eCOAs). Clinical Research is subject to international, European and national regulations.

(4) Clinical Study Data

All data collected for the purpose of a Clinical Study, including data from Healthcare Professionals and from Study Subjects. Such data may include Personal Data as per GDPR Article 4(1) as well as health data that are classified as special categories of Personal Data as per GDPR Article 9.

(5) COSUP (Supervisory Committee)

Internal body of the European CRO Federation (EUCROF), accredited by the competent supervisory authority specified in section 1.7 hereafter, vested with the required capacities to monitor the effective implementation of this Code of Conduct.

(6) CRO – Contract Research Organisation

A Contract 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 (interventional or observational) as well as other activities in connected domains.

Notes:

- 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.
- CROs are directed to consider the definition of data processor in Article 4(8) of the GDPR with regard to their role in processing Personal Data for Clinical Research, in particular that the data processor shall process Personal Data on behalf of the data controller.
- If a CRO has the status of an Investigational Site, the services and activities of such CROs related to that status are explicitly excluded from the scope of this Code.
- CRO staff may provide services that should be performed at the Investigational Site, physically or remotely. Such activities/tasks are normally required as part of site selection (initiation), site monitoring, on-site audit, on-site Investigator / site team meetings, direct-to-patient services etc. (See Appendix 2 Classes of services in scope of this Code.) A CRO shall at all times act on behalf of the Sponsor and upon Sponsor's authorisation and under their instruction, but the tasks shall be performed under the day-to-day supervision of the Investigational Site.
    - Example

      A CRO provides Investigational Site management services to the Sponsor and provides seconded personnel who work directly at the Investigational Site, performing activities for the Clinical Research normally performed by investigative team members e.g., Study coordinator. The personnel are under the day-to-day supervision of the Investigational Site and could either use a mixture of technology systems of the Investigational Site and the CRO, or just the systems of the Investigational Site. The seconded staff are employed by the CRO not the Investigational Site though and are providing the service to the Sponsor. Therefore, the CRO is not considered to have the status of the Investigational Site but are service providers acting under the direction of the Sponsor.

In this Code of Conduct, the terms "Service Provider" and "CRO" shall be understood as perfectly equivalent. For simplicity, "CRO" will be used in all subsequent sections of this Code of Conduct and shall be understood as meaning Service Provider for Clinical Research.

(7) EUCROF Code Compliance Mark

This is the badge or mark that a CRO can display once it has received approval from the COSUP as an adherent CRO to this Code.

(8) Exporter

Exporters means Sponsors or Service Providers (CRO or sub-processors) participating in an International Transfer of Personal Data as transferors of Personal Data.

(9) Healthcare Professional (HCP)

In the context of this Code, also referred to as Investigative team members, HCPs are natural persons who collect data, direct, or supervise the performance of a Clinical Study. Medical Doctors acting as Investigators, principal investigators, sub-investigator, coordinating investigator, as well as Study coordinator, sub-investigators, on-site data managers, pharmacists, Study nurses, lab technicians, and other members of the Clinical Study team acting under the responsibility of the Investigator are examples of such Healthcare Professionals. The primary responsibility of HCPs is to deliver care to the patients and therefore, as members of the wider team of HCPs, they act as data controllers for their medical care related processing activities. For the purpose of Clinical Study-related processing activities, the involved HCPs collect the Clinical Study Data of Study Subjects, as required by the Clinical Study's purpose and in compliance with the protocol. They are also data subjects for the CRO and/or Sponsors as these entities need to process their Personal Data to carry out the Clinical Study.

(10) Importer

Importers means Sponsors or Service Providers (CRO or sub-processors) participating in an International Transfer of Personal Data as receivers of Personal Data.

(11) International Transfer

International Transfer of Personal Data means sending or transmitting Personal Data to recipients located in Third Countries by any means (including but not limited to by post or e-mail) or by otherwise making Personal Data actually accessible to recipients located in Third Countries (e.g., by uploading Personal Data electronically in a database in which persons located in Third Countries will actually have access, or by granting them remote access to a database located in the EU).

(12) Investigational Site or Investigator Site

An Investigational Site is a healthcare provider organisation, public or private, participating in a Clinical Study in the frame of a contract with the Study's Sponsor.

(13) Investigator

A researcher involved in a Clinical Study. Related terms include site principal investigator, site sub-investigator, Study chair, Study director, and Study principal investigator.

(14) Personal Data

As per GDPR Article 4(1), Personal Data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

In this Code, Personal Data are data relating to the data subjects involved in Clinical Studies, primarily the Healthcare Professionals and Study Subjects, as well as personnel of the CRO and Sponsor to the extent they are used in the context and for the purposes of the Clinical Study.

(15) Primary use of Clinical Study Data

All processing operations related to a specific Clinical Study protocol during its whole lifecycle, from the commencement of the Study to deletion at the end of the archiving period, including the submission of data in marketing authorisations or reimbursement decisions.

(16) Pseudonymisation

As per GDPR Article 4(5) pseudonymisation means the processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person.

As per GDPR Articles 25(1) and 89(1), the application of pseudonymisation to Personal Data can reduce the risks of subject re-identification to the data subjects concerned and help controllers and processors to meet their data protection obligations.

(17) Secondary use of Clinical Study Data

For the purpose of the Code, this means further processing, for scientific research purposes, of Clinical Study Data for another purpose than the one described by the protocol, which is considered the Primary use of Clinical Study Data. Collection of additional data that may occur within the extension of the same protocol, e.g., as a result of a protocol amendment, shall not be considered Secondary use of Clinical Study Data.

(18) Sponsor

A Sponsor is the legal entity that takes responsibility for the initiation, management, and/or financing of a Clinical Study. It is the legal entity that defines the purpose and the means of a Clinical Study and is therefore acting as a controller according to GDPR Article 4(7).

Examples:

- A Sponsor may be a private company (Pharmaceutical Laboratory, Medical Devices Manufacturer, Biotech, private hospital or clinic) or an Academic Institution (Public Research Organisation / Institution, public hospital, Medical non-profit Association or Foundation).

Note:

- A Sponsor in the context of this Code could itself be party to a joint controller relationship with another data controller such as a second Sponsor. In this case, the provisions of this Code can still apply to the processing performed by the CRO acting as data processor for the data controller(s). The Data Processing Agreement shall specify the distribution of the controller's roles and responsibilities between the joint controllers vis-à-vis the CRO. For example, it could be the case that only one of the data controllers contracts with and instructs the CRO. Alternatively, the joint controllers may jointly contract with and instruct the CRO.

(19) Study Subject

A human individual who has volunteered to participate in a Clinical Study whose Personal Data is processed by the CROs and Sponsors and is a data subject as per Article 4(1) of the GDPR; "*an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, (…)*". The term Study Subject also covers human individuals other than Healthcare Professionals whose data may be collected in the context of a Clinical Study, such as the pregnant partner, newborn child or other family members acting as caregiver.

(20) Third Country

Means any country outside the European Union (EU) and the European Economic Area (EEA).

1.5 Business Rationale

A Code of Conduct dedicated to CROs is justified for the following reasons:

- CROs participate in processing Personal Data in the context of Clinical Research as data processors, at any point from the conception phase of the Clinical Research to the archiving phase;
- CROs perform processing operations on large volumes of Personal Data with specific software dedicated to Clinical Research, including processing of special categories of data within the meaning of Article 9 of the GDPR;
- CROs bear a pivotal role between the different actors involved in Clinical Research and notably between Sponsors, Investigational Sites and supervisory authorities; and
- A considerable amount of CROs are micro, small and medium-sized companies, whose resources might be insufficient to carry out their own analysis of the application of the GDPR to their data processing activities in the Clinical Research sector.

Development of the Code was triggered by the clear identification of the lack of harmonised approaches with regards to the application of the requirements of the GDPR to the data processing in which CROs are engaged.

Inviting CROs to comply with the requirements established by the Code promotes better safeguards for data subjects in Clinical Research. A Code of Conduct contributes to transparency of the practices employed by CROs and also offers better protection for data subjects if the adhering CROs implement the principles of the GDPR. The effectiveness of the Code shall be guaranteed by the continuous supervision by the dedicated Code's monitoring body accredited by the Code's lead supervisory authority that approved the issuance of the Code.

The demand for a Code for CROs was scrutinised in discussions with privacy and clinical experts, confirmed and recognised by the authorities, including by the representative of the European Data Protection Supervisor (EDPS). Clinical Research is mentioned twice in the EDPB Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies as a domain that should benefit from a Code of Conduct being developed.

Several essential problems for CROs have been identified:

1) Article 32 requires processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. CROs apply their own judgment which leads to inconsistency of risk estimation. Risk evaluation is not entirely objective. By experience, it depends

on whether a CRO is a single-service or a full-scope service provider, what type of services it delivers, and whether the CRO has only local or global outreach. Consequently, different organisations evaluated the risk of essentially similar activities in the similar context quite differently.

A reliable method to standardise assessment of what measures are appropriate is an ISO certification. Obtaining ISO certifications is often not feasible and/or appropriate, especially for SMEs/start-ups. The Code provides CROs with a practical tool allowing them to define the services, data processing context, the associated risk, and link these factors to the technical measures that are necessary to manage the risks in a consistent way according to a consensus developed by experts in the industry. This shall harmonise and reinforce the mandatory minimal level of protection of Personal Data offered by the adhering organisations.

2) Article 28 requires controllers to use only processors providing sufficient guarantees to implement appropriate technical and organisational measures. This requirement results in an exposure of processors to repetitive and heterogeneous processor assessments from different clients (controllers). Due to the absence of an agreed industry standard of what are appropriate security measures in application to Clinical Research, controllers (Sponsors) apply various in-house matrices generated based on their internal evaluation of their business risks and expectations towards the CROs. As a rule, Sponsors do not accept representations of GDPR compliance developed by a CRO and instead require CROs to be evaluated according to their own standards.

   With such a disharmonised approach from Sponsors, CROs have no possibility to standardise their own internal processes. The EUCROF Code helps to address those issues and companies would be able to better focus on coherent and proportionate implementation and improvement of measures. Article 28(5) GDPR specifies that adherence to a Code can be considered as providing sufficient guarantees. A CRO that has obtained a EUCROF Code Compliance Mark can use it as evidence of compliance recognised by the supervisory authorities with no need to complete numerous questionnaires. The resources spared by both controllers and processors can be invested in better compliance or monitoring of compliance instead.

3) CROs use their own judgement to develop processes that enable them to achieve and demonstrate compliance with GDPR. However, regardless of these compliance efforts, the supervisory authorities may apply penalties to such CROs if they are found in a breach of compliance with the GDPR, e.g., in the course of a supervisory authority's inspection, etc. However, if the CRO adheres to a Code of Conduct then this will be considered by the supervisory authorities when deciding whether to impose an administrative fine and deciding the amount of the administrative fine as per Article 83(2)(j) GDPR. This can mean that those CROs that have not attempted compliance with this Code can suffer a financial impediment compared to adherents of the Code, which is a strong incentive for CROs to adhere to the Code.

   The EUCROF Code offers a clear mechanism of adherence and related verification and operates as a rulebook for processors who design and implement GDPR compliant data processing activities, which is in line with Guidelines 1/2019. As the Code gains momentum and recognition in the industry it will become an expectation that CROs adhere to it and thus the general state of compliance in the industry will be improved as incentives for compliance increase.

The present Code provides standardised operational procedures and mechanisms to facilitate CROs' compliance with the requirements of the GDPR with the consideration of the specific characteristics of the processing carried out in the Clinical Research sector and, in particular, the needs of micro, small and medium CROs.

1.6 Purpose

To realise the identified business rationale, this Code of Conduct aims to:

- 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[2], 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

[2] 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.

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[3];

  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 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.

The Code of Conduct is thus drawn up to reconcile the protection of the privacy of individuals participating in Clinical Research with the conduct of that research by CROs and the free circulation of data essential to the pursuit of such activities and the economic development associated with it.

1.7 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 considering 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 to assist organisations and companies with GDPR compliance.

Even though the CNIL was the competent authority to manage the application procedure for submission of the Code, this is without prejudice of the powers given to all supervisory authorities by GDPR and the supervisory authorities retain all powers granted to them under Article 55 of the GDPR.

1.8 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.

Appendix 1 lists all concerned data protection supervisory authorities.

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.

Without prejudice to the concerned parties' responsibilities to fulfil their separate obligations in relation with GDPR, the following are excluded from the scope of this Code; (a) all processing activities carried out by both Sponsors and CROs that fall outside this contractual relationship, and (b) processing activities performed by

[3] 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 14th December 2022.

the CRO as a data controller in its own right.

The types of Services in the scope of this Code are described and listed in Appendix 2.

Note:

- Because the descriptions of the Services in this Appendix 2 have a generic value, they are hereinafter also referred to as "classes of services".

Such Services may concern any type of Clinical Studies as defined in section 1.4 (3) of this Code, including interventional and observational studies, as well as primary and secondary use of Clinical Study Data as defined in section 1.4 (15-17).

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.

Personal Data of the personnel of the CRO and Sponsor shall be considered in the present Code of Conduct only to the extent they are used in the context and for the purposes of Clinical Research. Other purposes of processing, e.g., for general staff administration, are the separate responsibility of each party and shall not be considered in scope of this Code of Conduct.

Notes:

- A legal entity acting as processor for another 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.
- A CRO not established in the European Union is eligible for adherence to this Code to the extent that the processing activities covered by the Code are subject to the GDPR under Article 3(2), such CRO shall be expected to demonstrate compliance with the requirements of Chapter V of the GDPR and section 4.6 of this Code.
- A legal entity falling within the definition of CRO which is not a member of EUCROF is eligible for adherence to this Code of Conduct and the fees paid for adherence will not confer membership to EUCROF.
- This Code of Conduct does not necessarily intend to cover all potential processes that could be implemented in the frame of a Clinical Research project or programme. In such situations, for a process that falls outside the scope of this Code of Conduct, the CRO and the Sponsor retain the discretion to conclude special and adapted contractual arrangements for the purpose of that specific process.

1.9 The data processor role

1.9.1 Rationale in this Code

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 Sponsors and CROs or multiple CROs 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 the role of data controller for the Clinical Research and the subcontracted CRO adhering to this Code is acting as a data processor.

Whatever the role of the Healthcare Professional (HCP) and Investigational Site vis a vis the Sponsor, this Code shall apply in the same way since the GDPR role of the HCP or Investigational Site does not impact the compliance of the CRO with this Code. If the Sponsor instructs the CRO to contract on its behalf with the HCP or Investigational Site then the CRO shall still be considered the Sponsor's processor and the Code shall apply.

1.9.2 Exclusion from this Code of Conduct

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.

The stakeholders of Clinical Research, particularly Sponsors and CROs, always have the possibility to engage each other in relationships where the controller / processor responsibilities may have a different split than in this present Code.

Examples:

- The Sponsor and the CRO are engaged in a contractual joint-controller relationship..
- Sponsors and the Investigational Sites are excluded.
- A CRO that provides a service that is not covered by the Classes of Services of this Code.

This Code of Conduct does not apply to such cases.

This does not mean that such situations may not happen. If such situations happen, the organisations concerned shall set up the appropriate contractual conditions and measures and those conditions are not governed by this Code of Conduct.

Generally, adherence to the Code does not prevent an organisation from complying with the GDPR for activities that may be carried by those organisations, and which are not governed by or included in the scope of the present Code of Conduct.

1.9.3 The non-exclusivity and non-equivalence principles

The fact that this Code only considers contractual patterns where the Sponsor is the controller and the subcontracted CRO a processor, does not prevent the subcontracted CROs from carrying out activities for which they have the role of data controller, nor does it exclude the possibility that the same organisation may run different activities for which it may have different roles.

Examples:

- Certain activities where the data subjects are personnel of the CRO and the activity relates to the general management of said personnel, are activities where the CRO is acting as data controller.
- A CRO building and maintaining databases containing information about Healthcare Professionals that can be invited for participation in any future Clinical Research not yet the subject of a contract with any Sponsor, acts as data controller with respect to that specific processing activity.

Without prejudice of an *ad hoc* assessment by any supervisory authority, the fact that a CRO carries out processes for which it acts as a controller outside of the Service Contract cannot be interpreted to reframe the position of that said CRO as a joint-controller in the frame of the Service Contract.

1.10 Compliance Principles and Methodology

1.10.1 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.

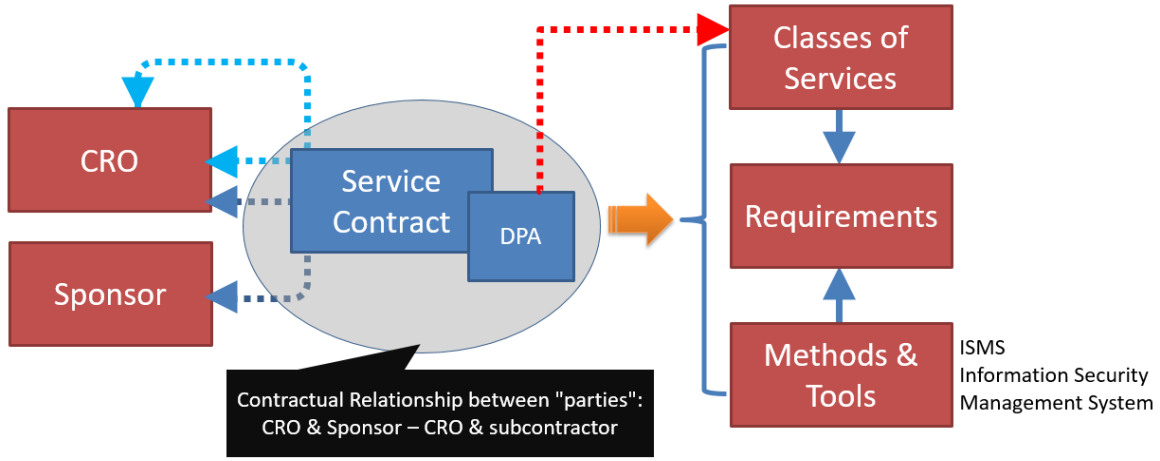
The conditions concerning Data Protection laid down in the Service Contract altogether constitute the Data Processing Agreement (DPA) between the parties to the Service Contract. These conditions can be included

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 the 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.

1.10.2 A compliance scheme adapted to each company profile: Statement of Applicability

This Code establishes a list of requirements against which compliance is assessed and monitored.

In total, 216 requirements have been specified and listed: 91 are specific of this Code and are specified in this document; 113 correspond to the control requirements of ISO 27001 standard and 12 correspond to the control requirements of ISO 27701 standard.

CROs may fall into 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 Clinical Research domain. Therefore, the Code has been designed to reflect that the compliance model for one CRO adhering to the Code may be quite different from another CRO adhering to the Code.

This means that a small CRO delivering one single service with limited impact in terms of data protection[4] and no dedicated online IT Platform does not need to comply with all 216 requirements.

Compliance to this Code depends on the CRO's profile defined by the classes of services the CRO sells to its clients, be they Sponsors or other CROs. If a CRO delivers a wide range of services, it can apply for adherence for all, one, or several selected services.

Appendix 2 hereinafter lists all classes of services in scope of this Code. The term "class" refers to the fact that these services are described in a "generic" way and are not specific to the particular methods / deliverables developed by one given CRO.

[4] For example, *Synopsis, protocol and CRF design* or *Site selection and contract*

Therefore, the first requirement of the Code specifies as follows:

> **1.10.** An adherent CRO shall define a Statement of Applicability listing all classes of services for which the adherent CRO declares compliance with the Code.

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

Document 02 of 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		
...	…		…		

Example of a CRO delivering services in classes 1 (Synopsis, protocol and CRF design) and 3 (Site selection and contract).

This approach enables a CRO to drop all requirements that are not applicable for the adherence of the particular CRO. It facilitates adherence by CROs falling under the definition of small and medium enterprises as defined by the European Commission[5].

This Code considers that full services CROs seeking adherence for all listed Classes of Service shall comply with all applicable requirements of the Code. ISO 27001 certification is highly recommended but not mandatory.

Requirements corresponding to the Statement of Applicability of an adhering CRO have a binding force and therefore contractually engage the responsibility of that said CRO to be compliant with those requirements during their period of adherence to the Code.

A CRO adheres to the Code, when it demonstrates compliance with all listed requirements corresponding to its company profile (i.e., Statement of Applicability). This implies documenting how the CRO complies with each of the applicable requirements. When appropriate, this may require the attachment of additional documentation such as SOPs, standard operating procedures (SOPs), policies or specific records, and documentation pertaining to an Information Security Management System (ISMS).

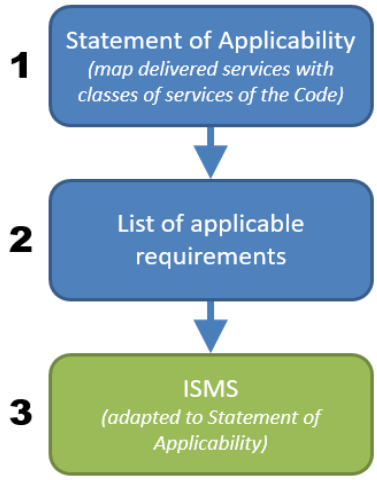
1.10.3 Information Security Management System (ISMS)

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 (QMS). They are accustomed to the collection of the necessary corresponding records to demonstrate throughout time, the maintenance of such QMS and its continuous improvement.

In common with any compliance process, the methods of compliance specific to the CRO shall be appropriately documented and monitored by means of records.

Under this Code, compliance with the security obligations of processors shall be realised by means of an ISMS – Information Security Management System such as those exemplified in the ISO 27001 and ISO 27701 standards (refer to section 4.2 of the Code for more details).

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



The left figure illustrates the 3 main steps to apply the ISMS:

1 Establish the "Statement of Applicability" of the CRO by mapping the delivered services with the classes of services in Appendix 2 of the Code;

2 Analyse document 02 of the Code to obtain the list of requirements of the Code applicable to the CRO. If any requirement shall be excluded they must be listed and justified as per requirement 4.2.e;

3 Document compliance measures by means of an Information Security Management System (ISMS) corresponding to the Statement of Applicability and maintain such system throughout time (refer to section 4.2 of the Code for more details).

1.10.4 Compliance Marks

As a result of its adherence, a CRO receives the right to display a EUCROF Code Compliance Mark. The Code provides for two different levels of adherence, to which correspond two distinct Compliance Marks. As further described in Section 5 of the Code, CROs have the possibility to choose what level of adherence they would like to pursue.

A Level 1 EUCROF Code Compliance Mark is awarded to a CRO that has successfully passed a review by the COSUP in the declarative adherence procedure, and a Level 2 EUCROF Code Compliance Mark is awarded to a CRO that has, in addition, successfully passed an assessment done by an external auditor.

To obtain either of the Compliance Marks, the CRO must demonstrate compliance with the Code requirements that apply to their Statement of Applicability.

When interpreting the Compliance Mark a CRO has obtained, Sponsors and other stakeholders should consider the complexity of evaluation that is associated with each level, as well as the amount of resources that a CRO would be expected to invest into the assessment process.

2 General Frame for Data Protection

2.1 Data Subjects

The present Code defines the rules for the processing of Personal Data of the following groups of individuals:

1) Study Subjects
2) Healthcare Professionals
3) Other Study stakeholders

Study Subjects include pregnant partner, newborn/unborn baby of the Study Subject, and relatives/family members, e.g., when a Study envisages research on genetics and heredity.

Healthcare Professionals includes the Investigators, Study coordinators, nurses, and other personnel who are directly engaged in the Clinical Research.

Other Study stakeholders may be contributing to the research and therefore, their Personal Data may also be captured in Study-related documents. These individuals may include personnel of the Study Sponsor, personnel of the CRO, representatives of health authorities, patient representatives, medical advisors, members of Data Safety Management Boards, and representatives of ethics committees.

2.2 Sources of data processed

2.2.1 Study Subjects

Depending on the purpose of the Clinical Research and Sponsor's instructions, including as specified in the Service Contract, CROs may receive data of the Study Subject from:

- Healthcare Professionals;
- Study Subjects themselves, e.g., through Patient Reported Outcomes;
- Study Subject's legal representatives;
- Study Subject's relatives/family members, e.g., through a questionnaire;
- Databases and/or collections of biological samples, legally constituted and, when applicable, having undergone the necessary formalities with the competent authorities or for which use/access is legally authorised. Such resources may be accumulated as a result of Clinical Studies in which Study Subjects granted their consent for the use of their leftover biosamples and other data generated in the course of the "main" Study for future Research purposes.

As per the definition of Study Subject in this Code, the scope of Personal Data may additionally include the data of other individuals, such as the pregnant partner, newborn child or family member acting as caregiver of the subject participating in the Clinical Research. This means that in the context of Clinical Research and as provided in the Data Processing Agreement, the CRO may be collecting the data of such individuals. The data from these individuals may be collected directly or indirectly from the Study Subject participating in the Clinical Research.

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[6] per Article 4(5) of the GDPR.

CROs may also process directly identifying Personal Data for supplementary services, as instructed by the Sponsor, and under the condition of appropriate safeguards in accordance with section 3.6.3 of this Code. These types of data can be collected from the Healthcare Professional or the Study Subject themselves.

Example:

A CRO delivering a service of patient reimbursement for expenses related to traveling and accommodation for the time of visits to the hospital, will need to collect directly identifying Personal Data of Study Subjects, such as name, contact data, travel information, etc. In this case, a CRO either should not be delivering the services that imply parallel processing of data concerning health or should

[6] Article 29 Working Party's Opinion 5/2014 on Anonymisation Techniques or any subsequent version thereof

implement additional technical and organisational security measures as per section 3.6.3 of this Code. Those safeguards are intended to ensure the confidentiality of the Study Subject and create appropriate firewalls between personnel who need to process directly identifying Personal Data and those personnel who should only process the pseudonymised Personal Data. More information on direct-to-patient services is also provided in Appendix 2 Classes of services in scope of this Code.

2.2.2 Healthcare Professionals

Personal Data of Healthcare Professionals (HCPs) are necessary for the Sponsor to assess whether the professional qualifications and experience of the HCP corresponds to the Study needs. A Sponsor may also collect Personal Data that are necessary for communication with the HCPs, arrangement of Study-related shipments to the Investigational Site and Investigator meetings, etc. When CRO processes Personal Data of HCPs who are involved in the Clinical Research, such data will include directly identifiable data limited to what is necessary for the defined Study-related purposes. Obviously, the scope of data shall not include health-related data, unlike in the case of data processing applicable to Study Subjects. The data relating to Healthcare Professionals involved in the Clinical Research comes from the individuals themselves or from other parties directly involved or/and having the knowledge and legitimate professional and business interest in providing such information for the purposes of Clinical Research. When a Sponsor engages HCPs into their Research, the Sponsor is obliged to inform the HCPs about the intended or actual data processing.

Examples:

- Sponsor engages a CRO to recruit Healthcare Professionals and provides the CRO with the Sponsor's database of Healthcare Professionals that they maintain as internal resource; the CRO and Sponsor contractually agree that the CRO shall develop data protection notices and provide them to the HCPs on behalf of the Sponsor.
- A Healthcare Professional may recommend a colleague who possesses relevant professional experience and qualifications and who may be potentially invited to be a Investigator team member; the sponsor/CRO shall receive from the HCP only the contact information of the referred colleague, all other data necessary for the Clinical Research shall be obtained directly from the referred HCP.

In both examples the Sponsor is responsible for the notification to the HCPs. However, in the first example it is appropriate to align the contents of the data protection notice with Article 14 of the GDPR. In the second example, the contents of the notice shall be aligned with Article 13 of the GDPR. Further guidance can be sought in section 3.1 of the Code.

2.2.3 Other Study stakeholders

When CRO processes Personal Data of other Study stakeholders who are involved in the Research, such data will include directly identifiable data but not health data. Normally the data will be received either directly from the individuals involved or from the organisation that employs that individual.

The Personal Data of these individuals is used for the purpose of business communication; e.g., project team reports to the personnel of the Sponsor on Study progress, operational control over the conduct of the Study, e,g., CRO assigns its personnel with the responsibilities to facilitate the conduct of the Study, performing administrative and regulatory functions, e.g., project teams make submissions to ethics committees, and other communication, CRO's sub-processors provide the Healthcare Professionals and Sponsor personnel technical support for the software used in the Research.

2.3 Accountability & liability

The Sponsor, as a data controller, is responsible for being able to demonstrate compliance with the GDPR (principle of Accountability) and this responsibility extends to its subcontracted CROs acting as processors who have their own liability under GDPR (e.g., Article 82(2)).

For such subcontracted CROs and based on (a) the publicly available Statement of Applicability of that said CRO and (b) the Service Contract and attached Data Processing Agreement listing the subcontracted services, adherence to this Code shall be considered as one element to demonstrate that the CRO complies with the applicable requirements of the GDPR.

Where the CRO engages another processor (sub-processor) to carry out processing activities on behalf of the Sponsor, the CRO still remains liable to the Sponsor for the sub-processor's activities.

Notes:

- What is required for the Sponsor to demonstrate accountability in accordance with GDPR is outside the scope of this Code.
- The CRO, as the data processor, shall follow the written instructions for processing provided by the Sponsor. Where the CRO deviates from those written instructions, the CRO is acting beyond the scope of a data processor and could be found to be a data controller.
- The CRO shall also be able to produce other documentation, such as the documentation maintained in the ISMS, to demonstrate compliance with the GDPR when requested by the Sponsor or another agent mandated and designated by the Sponsor and acting according to the audit conditions set out in the Service Contract and attached Data Processing Agreement. The documentation produced shall be limited to the scope of processing the CRO does for the Sponsor. As an example, the CRO shall not have to demonstrate compliance with its obligations under the GDPR in terms of employment matters because the CRO is the controller for the Personal Data of its personnel.

2.4 Data processing clauses to Service Contracts

All activities performed by CROs (acting as a data processor, as detailed in the scope of this Code of Conduct) on behalf of a Sponsor (acting as the data controller) in the context of Clinical Research are governable by a contract between both parties that must comply with the requirements of Article 28 GDPR (hereinafter the "Service Contract").

The clauses regarding data protection complying with Article 28 GDPR are referred to in this Code as the "Data Processing Agreement".

The Data Processing Agreement can be a standalone document or form part of the main contract between the Sponsor and CRO. Regardless, the Data Processing Agreement shall be explicitly considered an integral part of the Service Contract and shall detail all obligations of the parties regarding the appropriate handling of Personal Data as required by the GDPR and this present Code of Conduct.

Application domain: Requirements explained in each section of this chapter apply generally, i.e., to all classes of services listed in Appendix 2, except classes (1) and (2).

2.4.a A legally-binding Data Processing Agreement shall be entered into between the CRO and the Sponsor in writing.

2.4.b The Data Processing Agreement shall be explicitly considered an integral part of the Service Contract and must be signed before any data processing activity is performed by the CRO on behalf of the Sponsor in the context of the Clinical Research.

2.4.c The Data Processing Agreement shall detail all safeguards required for the protection of the Personal Data in accordance with Article 28 GDPR.

In the case where there is a Master Service Agreement (MSA) valid for all projects on which the CRO works for the account of the same Sponsor, a specific Data Processing Agreement shall not be required for each new work order issued by the Sponsor under this Master Service Agreement. However, the detail of the Nature of Processing, Categories of Data Subjects, Categories of Personal Data Processed, sub-processors, Technical and Organisational Measures, and Details of International Transfers, shall be required to be adapted for each processing activity that the CRO is contracted to perform. It is acceptable for these details to be included in a work order that falls under the Master Services Agreement, rather than in a Data Processing Agreement that is part of the Master Services Agreement. Such work order should reasonably address requirements of Article 28(3) of the GDPR.

Examples:

- A CRO provides monitoring and data management services to a Sponsor and this activity has been contracted globally under a Master Service Agreement. This MSA foresees that a specific work order shall be placed by the Sponsor each time the CRO

participates in a new Clinical Study. The contractual set-up should include a Data Processing Agreement as an integral part of the MSA and the specific conditions that apply to any specific contracted activities shall be included in the work order.

- A CRO provides to a Sponsor an IT platform in a Software as a Service mode (including training, user support and software maintenance activities for instance) and this activity is subject to a global Service Contract. This global Service Contract may include the Data Processing Agreement. The provisions of the Data Processing Agreement would cover all Clinical Research performed by the Sponsor using the IT platform and there is no need for a specific Data Processing Agreement for each separate Clinical Study performed by the Sponsor using this IT platform.

Model Data Processing Agreements offered by EUCROF may be inserted into Service Contracts where the parties are respectively data controller / data processor and data processor / sub-processor. These documents are provided as non-mandatory examples and can be used as a binding written basis for the distribution of responsibilities regarding data protection, agreed between the parties to the Service Contract. Alternatively, a CRO may use its own templates of Data Processing Agreements, subject to the provisions of this Code.

Additional information about the conditions of use of these models of Data Processing Agreements are defined in an additional note that can be downloaded from EUCROF website by CROs filing for adherence. The model Data Processing Agreements offered by EUCROF are designed as standalone documents.

The main requirements for any Data Processing Agreement are listed hereafter:

2.4.d The Data Processing Agreement shall delineate the roles and responsibilities of both parties.

2.4.e The Data Processing Agreement shall be valid for the entire duration of the provision of Personal Data processing services by the CRO and cannot be terminated unless other agreements governing the provision of Personal Data processing services have been agreed between the CRO and the Sponsor or the services are terminated. The Data Processing Agreement should include a requirement for the survival of confidentiality obligations after termination, as long as they do not apply to the legitimate requests for disclosure from data protection supervisory authorities.

2.4.f The Data Processing Agreement shall clearly identify the processing activities that are being covered.

2.4.g The Data Processing Agreement shall clearly define the data processor's responsibilities to answer data subject requests, taking into account the requirement under section 3.6.1.a of this Code, and detail the technical and organisational measures required to be put in place by the CRO to assist with the Sponsor's obligation to respond to requests for exercising the data subjects' rights.

2.4.h The Data Processing Agreement shall specify that the data processor cannot use the Clinical Study Data for its own purposes.

2.4.i If the data processor considers that an instruction of the data controller infringes applicable laws and regulations, the Data Processing Agreement shall specify that the data processor shall inform the data controller and cease to follow / apply such instruction.

2.4.j The Data Processing Agreement shall clearly identify the assistance that the data processor will provide to the data controller under Article 28(3)(e) to (f) of the GDPR; including:

- The data processor shall help the data controller in completing the data protection impact assessment (DPIA).
- The data processor shall be engaged to support the data controller in case a consultation of the concerned supervisory authorities is required prior to the completion of the DPIA.

2.4.k The Data Processing Agreement shall, in accordance with the provisions of Article 28(3)(a) of the GDPR, prohibit the data processor from transferring Personal Data to a Third Country without the prior written instructions of the data controller, unless data processor is required to do so by Union or Member State law to which the data processor is subject. The data processor shall be obliged to inform the data controller before processing, of the applicable legal requirements from Union or Member State law to which it is subject entailing the transfer of Personal Data to a third country or an international organisation, unless that law prohibits such information on important grounds of public interest.

The Data Processing Agreement shall contain instructions for transferring Personal Data to a Third Country[7] referring to the specific transfer mechanisms envisaged by Chapter V of the GDPR and that the data controller approves for use.

2.4.l The Data Processing Agreement shall identify the technical and organisational measures appropriate to protect Personal Data with the consideration of the specific risks of the processing to the rights of the data subjects, in particular of the Study Subjects whose Personal Data processed for the Clinical Research include special categories of Personal Data.

2.4.m The Data Processing Agreement shall include a requirement for the data processor to notify the data controller of any Personal Data Breach immediately after having become aware of such breach.

2.4.n The Data Processing Agreement shall specify that all Personal Data must be returned to the data controller, and that all existing copies must be destroyed by the data processor at the end of the Service Contract, or destroyed upon request and at the discretion of the data controller unless the CRO is subject to relevant obligations under Union or Member State law requiring the CRO to store Personal Data.

2.4.o The Data Processing Agreement shall impose a requirement for the data processor to train its personnel to handle Personal Data at least once a year and provide a training certificate that shall be included in the documentation package available in case of audit.

[7] EDPB Guidelines 05/2021 on the interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.

2.4.p The Data Processing Agreement shall oblige the data processor to make available to the data controller the list of its personnel authorised to access special categories of data processed under the framework of the Data Processing Agreement.

2.4.q The Data Processing Agreement shall oblige the data processor to obtain the individual confidentiality undertakings of the concerned personnel who process Personal Data that is subject to the Data Processing Agreement.

Note:

- Under the scope of this Code, in cases where the CRO is a party to the contracts with the Investigational Sites acting as processors, the Sponsor remains the data controller. In such contracts, the responsibility of the data controller cannot be transferred to the CRO who shall remain in its role of data processor. This note is without prejudice to the role of the Investigational Site under GDPR.

Example

- The incorporation of a confidentiality obligation clause in the employment contract (or freelancer's contract) can be one of the implemented measures.

2.5 Data processing clauses concerning sub-processing

In the context of a Clinical Research, the CRO may need to solicit its own sub-processors to meet the needs of Clinical Research and shall ensure its sub-processors commit to provide sufficient guarantees in line with Article 28(4) of the GDPR, as explained in section 4.4 of this Code, insofar as these service providers process Personal Data for the purpose of the Clinical Study. Examples of such sub-processors include centralised laboratories, the eCRF/ePRO solution providers, pharmacovigilance service provider, freelance monitor and biostatistician, company providing transport/logistics or archiving etc. In all such cases the Sponsor, as data controller, shall be given adequate notice of the CRO's intention to contract with a sub processor.

Example

- The CRO maintains a list of sub processors on its website including the date the list was last amended and sends a notification out to all Sponsors 30 days prior to a new sub processor being added, in order to give the Sponsor a chance to object to the addition of a new sub processor. In this example, the Data Processing Agreement must still be amended to incorporate the new sub processor as per requirement 2.5.b of this Code.

Application domain: Requirements explained in each section of this chapter apply generally, i.e., to all classes of services listed in Appendix 2, except classes (1) and (2).

The following shall also be covered in the Data Processing Agreement between Sponsor and CRO:

2.5.a The Data Processing Agreement shall include an undertaking not to subcontract any data processor activities without the prior written specific or general authorisation of the data controller and the execution of a contract with its authorised sub-processors that includes all applicable conditions of this Code of Conduct and specifically the commitments to provide sufficient guarantees in line with Article 28(4) of the GDPR[8]. Where specific authorisation is required, the Data Processing Agreement must include the process for obtaining such authorisation.

Note:

- Unlike with a specific authorisation, where a processor shall obtain controller's approval of each sub-processor, in case of a general authorisation the processor needs to inform the controller in due time of any intended addition or replacement

[8] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR

of sub-processor(s) so as to provide the controller with the opportunity to object. Controller's silence or/and failure to object within the set timeframe can be interpreted as authorisation.

2.5.b The Data Processing Agreement between the data controller and the CRO shall identify all sub-processors being appointed by the CRO as necessary for the delivery of its services and shall be deemed accepted by the controller upon execution of the Data Processing Agreement. Where additional sub-processors are envisaged after the Data Processing Agreement is signed, the controller must be informed or agree these in an amendment to the relevant agreement between the parties[9], depending on whether general or specific written authorisation of the controller was specified in the contract.

Note:

- The list of sub-processors shall be included in the Data Processing Agreement itself or in an annex to the agreement and kept up to date, in accordance with the general or specific authorisation given by the controller. Such list of intended sub-processors shall include per each sub-processor at least, their locations and type of services. Safeguards that have been implemented by the sub-processors shall provide for the equal level of protection as by the processor. A list of safeguards included into the Data Processing Agreement between the processor and controller shall be considered a proof of what safeguards have been implemented by the sub-processors.

2.5.c The Data Processing Agreement between the data controller and the CRO shall define the procedure to add / remove / change any of the listed sub-processors giving reasonable time for the data controller to consider any changes proposed by the CRO and object to new sub-processors.

The following shall be covered in the Data Processing Agreement between CRO and its sub-processor:

2.5.d The same data protection obligations as set out in the Data Processing Agreement between the controller and the CRO, as specified in section 2.4, shall be included in the contract between the CRO and its own sub-processors, in particular providing sufficient guarantees to implement appropriate technical and organisational measures as required by the GDPR and procedures to appoint further sub-processors.

2.5.e The Data Processing Agreement between the CRO and its own sub-processors shall clearly identify the processing activities that are being covered.

2.5.f The Data Processing Agreement between the CRO and its own sub-processors shall not permit the sub-processor to transfer Personal Data to a Third Country unless the sub-processor has implemented a legal mechanism for data transfer as per Articles 44-49 GDPR. In the case of any transfer (onward or otherwise) by its sub-processor, the CRO shall be responsible for ensuring that its sub-processor implemented a legal mechanism for data transfer and demonstrated the implementation of such safeguards before transferring any Personal Data to a Third Country, as per section 4.6 of the Code.

Note:

- When a sub-processor of the CRO fails to fulfil its data protection obligations, the CRO remains fully liable to the controller for the performance of that sub-processor's obligations. Nonetheless, this liability doesn't prevent the failing sub-processor from being directly sanctioned by data protection authorities. The CRO will be entitled to bring action against the failing sub-processor as well.

The following applies generally to subcontracting:

2.5.g The CRO shall provide a copy of the Data Processing Agreements between itself and the sub processors upon request from the data controller or the competent

[9] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR

supervisory authority, in order to demonstrate that there are sufficient guarantees in place.

2.6 Confidentiality obligations

Article 28 of GDPR foresees that […] *the processor ensures that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality*;

Application domain: Requirements explained in each section of this chapter apply generally, i.e., to all classes of services listed in Appendix 2.

2.6.a The CROs shall ensure that their employees are bound to a duty of confidentiality either in their employment contract, a separate confidentiality agreement, or any equivalent engagement mechanism, and are sufficiently informed and trained to exercise such duty in accordance with GDPR and corresponding company's standards and policies.

Notes:

- This requirement shall also apply in the case of freelancers and generally any sub-processors with whom CROs cooperate to provide the assigned services.
- See also requirements 2.4.o, 2.4.p and 2.4.q above.

2.6.b The CROs and sub-processors shall implement, document and monitor all technical and organisational measures to ensure that confidentiality obligations are appropriately followed by its employees.

Example:

- An employee handbook or similar document contains provisions on the disciplinary actions and sanctions that may be taken in accordance with the applicable labour law in case employees fail to comply with the duty of confidentiality. Sanctions or disciplinary actions may include verbal or written warnings, re-training, documented feedback from their functional manager, termination of the work contract (in compliance with the applicable regulation), or any other appropriate legal action undertaken by the employing organisation etc.

2.7 Instructions from the controller

Article 28 of GDPR specifies that […] *the processor processes the Personal Data only on documented instructions from the controller;*

Application domain: Requirements explained in each section of this chapter apply generally, i.e., to all classes of services listed in Appendix 2.

In this Code, the term "documented" shall only be understood as "written" (electronically or not) and with a clear identification of the controller authoring the instruction, as well as a clear identification of the Service Contract under which the said instruction is released.

If the Service Contract and corresponding Data Processing Agreement are designed to clearly establish the respective responsibilities of the parties (controller and processor) in a GDPR compliant manner, records shall be kept demonstrating that each party has continuously acted accordingly and that all essential instructions from the Sponsor / controller have taken a formal written form as required by GDPR Article 28.

In case of dispute or legal action, of inspections or in case of internal security audits, such records shall promptly be made available by the CRO.

As reminded in section 2.3 above (and provided that such instructions are compliant with the GDPR and laid down in the Service Contract) "*where the CRO deviates from those written instructions, the CRO is acting beyond the scope of a data processor and can be found as a data controller*".

Such records can be considered as part of the Trial Master File (TMF), be these instructions Study specific or not. Record means any written instructions provided by the Sponsor to the CRO, e.g., a memorandum, an e-mail or any other written means that can be attributable to the data controller. The term "essential" that is added here to define which instructions shall take such a written form, shall be understood with the same meaning as for the TMF, but it can be up to the parties to specify in the Service Contract or Data Processing Agreement which instructions shall take a written form and what shall be this form.

2.7.a CROs shall ensure that the processing of Personal Data performed under the Service Contract is only performed according to written instructions from the Sponsor acting in its controller role and that such written instructions are recorded in its documentation system and can be readily produced in case of audit.

Note:

- The CRO may include in its policies and standard procedures a list of all types of instructions that shall be obtained in writing from Sponsors, together with associated templates.

2.7.b CRO shall ensure that written instructions from the controller shall include at a minimum an unambiguous identification of the controller, of the Service Contract under which such instruction is released, as well as of the concerned process and / or service.

The reason for this requirement is that in case of inspection, dispute or legal action, the written document shall provide clear grounds for decision making and control.

Both the Sponsor / controller and the CRO / processor may have to face situations where a written instruction from the Sponsor is in scope of the Service Contract but its compliance with GDPR is possibly subject to different interpretations.

2.7.c The Data Processing Agreement signed by the Sponsor and the CRO shall provide a clear ruling on how to handle situations where a written instruction from the controller, as per section 4.5 of the Code is considered by the CRO as not compliant with GDPR or/and other Union or Member State data protection regulatory and statutory provisions. If such a case happens, the CRO shall have the option to obtain a written disclaimer to prevent any engagement of its responsibility or suspend the execution of the instructions in question until such instructions have been either clarified or amended to be in line with the GDPR or applicable regulations.

Notes:

- In all cases, such written instructions shall be in scope of the Service Contract.
- The written information released by the CRO to the Sponsor and the resulting disclaimer shall all be archived in the documentation system of the CRO and be readily made available in case of audit.

3 Application of the data protection principles to the activities of CROs

This chapter transposes in a practical manner and in the specific case of CRO activities, the general requirements of the GDPR. It is nevertheless recalled that, in all cases, adherence to the Code does not prevent a CRO from having to comply with all GDPR principles, including for its activities which are not governed by this Code of Conduct or included within its scope of application.

An adhering CRO must conduct its own legal analysis to determine whether there are circumstances other than those contemplated in this Code in which it should apply the principles of the GDPR.

3.1 Lawfulness, fairness and transparency

This section refers to Article 5 of the GDPR, which states that "*Personal Data shall be: a) processed* ***lawfully, fairly and in a transparent manner*** *in relation to the data subject* ("lawfulness, fairness and transparency") and Articles 12, 13 and 14 of the GDPR that define the information to be provided to the data subject.

To meet these obligations, the Sponsor acting as a data controller is responsible to provide detailed information to the data subjects about the processing of their Personal Data for the purposes of the Study, explain the legal basis for processing, obtain consent to data use if consent is the legal basis for data processing, and ensure that the fulfilment of these obligations can be demonstrated. The Sponsor can engage a CRO to provide the services and require the CRO to assist the controller in complying with these responsibilities.

Application domain. The requirements of this section apply for CROs delivering one or several of the following services listed in Appendix 2:

- (2) ICF design and information leaflet
- (3) Site selection and contract
- (4) Data collection
- (8) Patient services
- (22) Regulatory/Startup activities
- (23) Arrangement of Investigator meetings

To demonstrate accountability for compliance with the principle of transparency, a CRO shall develop a policy ensuring that the CRO shall assist the controller in providing complete information about data use to data subjects.

3.1.a Based on the information provided by the Sponsor, the CRO shall support the Sponsor in the development, communication/distribution of information about data processing to the data subjects and obtaining consent to the processing of Personal Data from the data subjects, when such processing relies on consent as the legal basis. All processes and documents developed by the CRO for the Sponsor shall be approved by the Sponsor before the CRO can use/release them.

3.1.b CROs shall have internal processes and procedures describing the distribution of the Sponsor´s privacy notices to Healthcare Professionals as part of feasibility, site initiation visits, etc.

Example:

- A CRO providing patient services (see list of services in Appendix 2) may have sample notices/consent forms developed to assist data controllers with meeting their responsibility related to informing data subjects about the processing of their Personal Data.
- A CRO who receives the Personal Data of Healthcare Professionals from a third party rather than the individual themselves will provide a privacy notice to that Healthcare Professional with, in particular, the source of the data and details on how to object to the processing of their data.

Legal basis for data processing and information to be given to data subjects

When a CRO is engaged in the development of Informed Consent Forms (ICFs) and information leaflets for

Study Subjects and in the selection of Healthcare Professionals, the CRO will defer to the controller's opinion on the appropriate legal basis for data processing as this is the responsibility of the controller to define. The CRO will include this information into the relevant sections of the ICF and information leaflets provided to the Study Subjects, and into the notifications to Healthcare Professionals.

3.2 Purpose limitation

This section refers to Article 5 of the GDPR, which states that *"Personal Data shall be: b) collected for **specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (**'purpose limitation'**);*

3.2.1 Primary use

The principle of purpose limitation sets the limits on the purposes for which Personal Data may be processed, given that according to this principle: i) Personal Data must be collected for specified, explicit and legitimate purposes and ii) not be further processed in a way incompatible with those purposes.

To demonstrate accountability for implementing the principle into the CRO's practices applicable to the delivery of services to the Sponsors, a CRO shall develop a policy addressing the purpose limitation principle and ensuring its implementation through the practices, procedures and data capture forms.

Application domain: Requirements explained in each section apply generally, i.e., to all classes of services listed in Appendix 2, except classes (1) and (2) and (17).

3.2.1.a Before commencing processing, the CRO shall check that all Personal Data to be processed by the CRO will be collected in accordance with the protocol of each Clinical Study.

Notes:

- A CRO is expected to review the protocol and compare the endpoints listed with the data points being collected and assess if there are any data points that do not pertain to the research protocol.
- A CRO delivering synopsis, protocol and CRF design services (see list of services in Appendix 2) is expected to incorporate in its policies and procedures provisions on how they train staff whose responsibilities consist of creating these documents for the service; such provisions shall explain the criteria, standards, and matrices for integrating the rules on controlling uses of Clinical Study Data by means of the design of those Study documents.

In the area of Clinical Research, the primary purpose for which Personal Data are processed is the attainment of the objectives pursued by the protocol of each Clinical Study. Thus, Primary use of Clinical Study Data includes all processing operations related to a specific Clinical Study protocol, during its whole lifecycle, from the starting of the Clinical Study to deletion, at the end of the archiving period.

3.2.2 Secondary use

Processing operations falling within this section are those that aim to use the Personal Data collected in the course of a Clinical Study for secondary purposes, namely for purposes other than the one defined by the Clinical Study protocol. Any Secondary use of Personal Data for scientific research purposes should be assessed by the data controller.

Examples:

- A Sponsor would like to use the medical data collected during a clinical trial on prostate cancer to run a Study aiming to identify new biomarkers, which was not foreseen in the Clinical Study protocol.
- A Sponsor decides to use pseudonymised Study data obtained during previous studies for scientific research, for instance for the development of new artificial intelligence algorithms, in order to enhance diagnostic approaches or disease assessment methodologies.

A data processor is not authorised to use the Personal Data it processes for secondary purposes unless instructed/authorised by the data controller. As per section 2.3, a CRO that acts beyond the controller's instructions may be construed to have assumed the role of data controller for the new purpose, meaning that it also must accept the obligations of a data controller and take steps to fulfil such.

3.2.2.a In cases where the CRO is instructed by Sponsor to process Personal Data outside of the original Study protocol, the CRO shall:

1) Ensure that the processing is performed in accordance with a contract that covers the secondary purposes of processing by amending the previous agreements or entering into new contracts; and

2) Adopt the suitable technical and organisational measures in this Code in order for the CRO to safely process Personal Data for secondary purposes.

Examples:

- A Sponsor decides to reanalyse data that was already collected and that this is a secondary purpose which is compatible with the original purposes according to the assessment of the controller. A CRO shall ensure that its processing is performed in accordance with an appropriate contract and fulfils its obligations thereunder, including, in particular, providing assistance to the Sponsor with the development and distribution of privacy notices to the data subjects as per Article 13 and 14 GDPR and in applying appropriate technical and organisational measures.

Secondary use of data that is fully anonymous, does not fall within the scope of this Code. Note that the process of anonymisation should also rely on a valid legal basis as per the Art. 29 Working Party Opinion 05/2014 on Anonymisation Techniques (or any subsequent version).

3.3 Data minimisation

This section refers to Article 5 of the GDPR, which states that *"Personal Data shall be: c)* ***adequate, relevant and limited to what is necessary*** *in relation to the purposes for which they are processed (****'data minimisation'****).*

The Sponsor acting as a data controller will require the CRO to align with the principles of data minimisation and privacy by design and default. Alignment with these key principles will help ensure the rights and freedoms of data subject are protected. Only the activities related to carrying out the Clinical Study or other services specified in the Service Contract with the Sponsor are within scope of these key principles.

In order to demonstrate the proper implementation of this principle in the context of the services provided to the Sponsor, the CRO must develop a policy addressing the principle of minimization aimed at ensuring its implementation through procedures and records.

Application domain: The requirements of this section apply to all classes of services in Appendix 2 with the exception of (17) Provision of physical hosting infrastructure or as listed in document 02.

Example:

- A CRO delivering synopsis, protocol and CRF design services (see list of services in Appendix 2) is expected to include special training on data minimisation for its employees; and offer a data minimisation analysis report in the deliverables provided together with the protocol and CRF design documents.

For the principle of data minimisation, the CRO shall only collect Personal Data that is adequate, relevant, and limited to what is necessary for the purposes they are processed. More specifically, the CRO shall only process Personal Data that is required to carry out the processing activities as instructed by the Sponsor.

3.3.a CRO shall support the Sponsor by only collecting Personal Data that is required as specified by the Sponsor's written instructions and the purposes at the time of collection. Any Personal Data not required to carry out the Sponsor's written instructions shall not be collected and processed by the CRO as a data processor.

3.3.b CRO shall provide, to the extent it is able within the area of its specific competence and expertise, any assistance sought by the Sponsor in defining the Personal Data that is adequate, relevant, and necessary for the purposes they are processed.

The Sponsor may require the CRO to provide tools to carry out processing activities as specified by written instructions. These tools may be created and maintained by the CRO or may be the product or service obtained from another party.

3.3.c For privacy by design and default, the CRO shall ensure that processing tools are able to support data minimisation principles, storage limitation requirements, and facilitate data subjects' rights as instructed by the Sponsor.

Notes:

- A CRO that provides an EDC system will design case report forms that technically do not allow Personal Data not required by the Study protocol to be entered e.g., by minimising free-text fields, including fixed fields instructing what types of data are expected to be entered, or having fields for entering year of birth or age rather than complete date of birth. This way, only the necessary Personal Data will be captured and unnecessary information which may contain special categories of Personal Data are not processed.
- When in the context of (23) "Arrangement of Investigator Meetings" the CRO is expected to ensure that all travel related documents, e.g., passport copies, visa applications, spreadsheets with travel schedules of the Healthcare Professionals are destroyed as soon as the meeting took place and the Investigators received compensation for expenses, so the Personal Data is not unnecessarily kept and thus exposed to unauthorised use or disclosure.

3.3.d The CRO shall require sub-processors whose applications/software is used to implement appropriate technical and organisational measures relative to the risk presented with the processing activity, and in particular that the tools have appropriate controls to limit access to only persons that are authorised to process Personal Data. As per Article 29 GDPR, any person who has access to Personal Data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Example:

- CRO engages a provider that hosts eTMF and arranges with the provider that the personnel of the provider do not receive access to the stored Study data, including Personal Data, but only accesses the user account information of the CRO staff to assist with the technical issues.

3.4 Accuracy

This section refers to Article 5 of the GDPR, which states that *"Personal Data shall be: …. c)* ***accurate and, where necessary, kept up to date;*** *every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (****accuracy****);"*

A CRO delivering services for Clinical Research, shall be able to demonstrate via its policies and data capture forms how it has integrated verification of data quality into its services provided to Sponsors. CRO will keep records in the Study files, implement and follow Sponsor's instructions for the relevant processes.

Application domain. The requirements of this section apply for CROs delivering one or several of the following services listed in Appendix 2 and as listed in document 02:

- (3) Site selection and contract
- (4) Data collection
- (5) Monitoring
- (6) Medical monitoring
- (7) Pharmacovigilance
- (8) Direct-to-Patient services
- (9) Data management
- (12) Financial management
- (15) Audits
- (16) Provision of IT managed services
- (20) Maintenance of Trial Master File (TMF)
- (22) Regulatory/Study start up services
- (23) Arrangement of Investigator meetings

Examples:

- If a CRO is engaged by a Sponsor for more than one Study, e.g., extension of a Study, where Healthcare Professionals are invited from the initial Study, a good practice would be that for the new Study/extension study a CRO requests confirmation from Healthcare Professionals whether the earlier obtained CVs, medical licences, other necessary documents from the other study can be used or the updated versions should be appropriate for regulatory submissions and TMF filing.
- A CRO delivering feasibility and Investigator selection service is instructed by the Sponsor to develop a database of all Investigators who are invited. Finally, such database will include the Healthcare Professionals who were selected and engaged, as well those who were not selected and not engaged but can be contacted for future studies by the Sponsor. Best practice would be to ensure that the Healthcare Professionals know the contact details of the Sponsor to communicate changes of their data or exercise data protection rights and if CRO receives any such information it shall communicate such to the Sponsor.

Further paragraphs of section 3.4 focus on ensuring accuracy to the data collected on Study Subjects.

3.4.1 Study set-up

The objective is to facilitate complete data collection and minimise data entry errors and the risk of deviations of Personal Data.

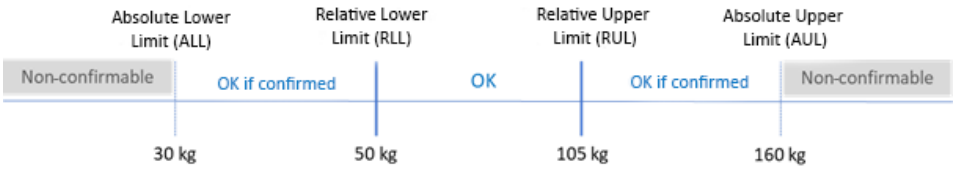
3.4.1.a The CRO shall set-up the data collection tools, including the Study database and Case Report Forms (CRF), so that data accuracy is facilitated and can be checked the earliest possible in the process of data collection.

Examples of types of controls that shall be implemented are the following:

- ***Data validation checks*** to ensure that the CRF only permits certain values and entries and that unstructured text variables are only used when duly justified.
- ***Format/type checks*** to verify that the data are collected according to the requested format/type: date format, coded, integer, etc...

  Example: A date requested in dd-mmm-yyyy format but completed as follows: 01-19-Mar, is rejected.
- ***Presence checks*** defining whether a variable is obligatory or not. It is also possible to notify about the absence of a variable but to confirm that this variable is not available.
- ***Plausibility checks*** to check whether a value is within the expected limits or not. Such checks can be defined at database set up. A distinction must be made between relative and absolute limits.

  Example for a patient's weight:



- ***Consistency checks*** aiming at detecting impossible or unlikely combinations of variables.

  Example: male sex and postmenopausal patient (impossible combination); female sex, age = 50 years' old and patient of childbearing age (unlikely combination).

- ***Date checks*** to check the chronology of dates in relation to each other.

3.4.2 Supervision of the collection of Personal Data

3.4.2.1 Data collection by Healthcare Professionals

3.4.2.a The CRO shall document the processes implemented to ensure accuracy during data collection, including the identification, roles and capacities of the people involved in these processes, to verify that no tampering is possible that might distort the accuracy of the data collection. In the case of a Study using an electronic CRF (eCRF), a CRO shall ensure that there are security measures and features of the eCRF tool that implement an adequate audit trail and controls to prevent interception or distortion while the data is in transit.

Examples of types of controls that shall be implemented are the following:

- In the case of a Study using a paper CRF, the measures implemented for the CRF management processes such as the following shall be described:

  Sending of CRF documents from the Study Investigational Site to the data entry office:

  - By electronic means: scanning and loading via a secure platform.
  - Transporting paper CRF: using a qualified and audited courier company implementing adequate security measures for the transport of paper CRFs.

- Follow-up of the CRFs received and check on receipt (e.g., number of CRFs received compared to the expected number).
- Data entry of data collected in the CRFs.
- Management of correction requests.
- Storage of paper CRFs in a secure file room.

3.4.2.b The CRO shall ensure that all measures to ensure accuracy are properly implemented throughout the lifetime of the Clinical Study and that such implementation is properly documented and regularly audited.

Examples of types of controls that shall be implemented are the following:

- In the case of a paper CRF, train the CRO data entry operators (training with fictitious documented patients, use of data entry guidelines, etc.) and adapt the data entry level to the Study (single data entry, double data entry with or without adjudication, etc.).
- Ensure that Personal Data is collected within the Study Investigational Site by qualified personnel, trained in the Study and the legislation in force (e.g., Good Clinical Practice, ISO 14155 standard, etc.).
- Ensure that staff in charge of data entry are authorised to do so by the principal Investigator, verification of task delegation (if applicable).
- Draw up and provide the centre with CRF completion rules (eCRF or paper CRF completion guide, video tutorial, FAQ, etc.).
- Ensure that the data are signed off by the principal Investigator certifying data accuracy; signature via eCRF and/or signature on paper CRFs prior to database freeze.
- Provide the eCRF login codes to the Healthcare Professional only after verification of their training and participation in the Study.

- Ensure that an audit trail system is available.
- Ensure that the list of eCRF users is regularly checked and filed in the Study TMF.
- If the requirements for setting up the database are met, the data entered will be checked automatically to detect missing, out-of-range and inconsistent data, according to the controls specific file and the annotated CRF validated during the database set-up phase (see section above).

3.4.2.2 Data collection from other sources

This section applies when external data (e.g., results of analysis of biological samples, imaging data, etc.), including so-called "source data" must be integrated in the Study database. The data must be integrated in such a way that ensures accuracy and completeness of the Personal Data, and correctly attributes it to the right Study Subject.

> **3.4.2.c** CRO shall draw up a specification document describing all measures and features for the set-up and processes to transfer external data and integrate them into the Study database. The specification document shall be brought to the knowledge of the sender of the data, prior to the receipt of these data by the CRO, in order to ensure that said measures and features are properly implemented by the sender.

This specification document shall, when appropriate, detail the following:

- The expected data type, format, sending frequency, etc.
- Secure data transfers from the source to the CRO: e.g., SFTP or HTTPS protocol, any other secure transfer process.
- Control procedures of the external data received before integration into the database; how is it ensured that the received data are compliant with the specifications.

There are cases where the data are directly uploaded into the database by the staff of the Investigational Sites or external providers, e.g., loading images or hospitalisation reports via eCRF, etc.

Such records or data sets may originally contain direct identifiers, e.g., name and birth date of a data subject.

> **3.4.2.d** CRO shall implement and document the process ensuring that the direct identifiers are removed from the health data of Study Subjects by the sender of the data prior to the receipt of these data by the CRO.

Note that in some cases, e.g., DICOM image data sets, pseudonymisation will be implemented at the time of upload into the eCRF, whether by automated or manual means. Such process shall be properly documented as per the requirements above.

3.4.3 Checking data

Application domain. The requirements of this sub-section applies only when the CRO oversees the monitoring (see Appendix 2, (5) Monitoring, (6) Medical Monitoring, (7) Pharmacovigilance) or is involved with the data management (see Appendix 2, (9) Data management).

> **3.4.3.a** The CRO shall detail in the Clinical Monitoring Plan or equivalent document all the processes related to checking Personal Data for accuracy and completeness.

> **3.4.3.b** The CRO shall ensure that the personnel in charge of the monitoring are qualified and known to the Sponsor. The CRO must maintain all appropriate documentation and records demonstrating that this requirement is properly implemented.

Examples of types of controls that shall be implemented are the following:

- CVs of the personnel in charge are regularly updated and checked.

- The personnel in charge are appropriately trained with Study training certificate available.
- The personnel in charge are made known to the Sponsor in a list of authorised personnel.

3.4.3.c The CRO shall, through the personnel in charge of the monitoring, check the accuracy and completeness of the Personal Data in accordance with the instructions of the Sponsor. The CRO shall raise any queries with the Investigational Site staff as soon as possible and ensure that these are resolved.

3.5 Storage limitation

Application domain. The requirements of this section apply to all classes of services in Appendix 2 with the exception of (1) Synopsis, protocol and CRF design, (2) ICF design & Information Leaflet and (13) Public disclosure.

This section refers to Article 5 of the GDPR, which states that *"Personal Data shall be: …. **e) kept in a form which permits identification of data subjects for no longer than is necessary** for the purposes for which the Personal Data are processed; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (**'storage limitation').***

In order to retain Personal Data as a data processor in accordance with Article 89(1) GDPR, the CRO must maintain compliance with this Code of Conduct and in particular its safeguards for the rights and freedoms of the data subject, including data minimisation and pseudonymisation, and the CRO must act under the instructions of the data controller.

To demonstrate accountability for appropriate data retention, a CRO is expected to include data retention and storage limitation provisions in the Data Processing Agreement between Sponsor and CRO; as well as developing the documents evidencing the return of Study documents with Personal Data to the Sponsor or the data destruction, e.g., instructions for TMF shipment, e-mail, forms acknowledging TMF receipt, document destruction forms/certificates, etc.

Examples:

- CRO providing data management services (see list of services in Appendix 2) develops data transfer specifications and files the evidence documents, including confirmation from Sponsor of receipt of the data.
- CRO providing decommissioning services (see list of services in Appendix 2) implements a contract governing the data deletion process and generation of data destruction certificates documenting due provision of the service.
- The Sponsor may request assistance from the CRO with inspections, processing for secondary purposes, etc., for this reason the Sponsor may instruct the CRO to keep Clinical Study data after the termination of the Clinical Study; for the time of retention the CRO shall ensure they are able to generate evidence for appropriate level of security for retention in archive, including access lists, physical security policy/applied standards for storage areas, etc.

3.5.a The CRO shall keep records documenting the instructions of the data controller in relation to data retention periods.

3.5.b The CRO shall implement the identified retention period to the data it processes on the instructions of the data controller unless an applicable Union or Member State law requires storage of the Personal Data.

3.5.c The CRO shall maintain compliance with this Code of Conduct for the entire time that it retains the data.

3.5.d The CRO shall ensure that where data is retained in archives, the technical and organisational measures implemented to protect such archived data are appropriate to the specific risks for the rights of the rights and freedoms of data subjects, and unless justified otherwise, shall enjoy at least the same level of protection as data retained in the non-archive storage locations.

3.5.e Adherence to the implemented technical and organisational measures shall be maintained for the entirety of the life of the archived data and the compliance of the archive shall be checked and re-certified at regular periods.

3.5.f The CRO shall, upon the controller's instruction, delete personal data that has reached the end of the agreed retention period. In addition, the CRO should put a process in place to delete any remaining legacy data for which it cannot identify a specified instruction. Data destruction 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.

3.5.g The CRO shall regularly review and identify data for which the retention period has expired. Such procedures can be manual but should be automated where technically possible.

Example:

- CRO implements a data discovery tool that finds and flags data for which the retention period recorded in the metadata has elapsed.

3.6 Integrity and confidentiality

This section refers to Article 5 of the GDPR, which states that "*Personal Data shall be processed in a manner that ensures appropriate **security** of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures* ('integrity and confidentiality')".

Application domain: The requirements of this section apply as per document 02 to all classes of services in Appendix 2 with the exception of (1) Synopsis, protocol and CRF design, (2) ICF design & Information Leaflet and (13) Public disclosure and (17) Provision of physical hosting infrastructure.

To meet this obligation, CRO must implement the necessary processes to maintain confidentiality and integrity of Personal Data of data subjects. To demonstrate accountability for the implementation of the principle, a CRO shall develop policy(ies) and ensure that the processes governed by the policies be monitored, audited, and documented through the relevant features of information systems of the CRO.

3.6.a A CRO shall develop privacy management policies and procedures, including appropriate controls, that will ensure the confidentiality and integrity of the Personal Data, in accordance with their evaluation of the risks inherent in the processing, and shall be able to demonstrate compliance with the technical and organisational measures implemented.

Notes:

Technical and organisational measures required to maintain confidentiality and integrity of the data are expanded upon in other sections of this Code, including:

A. Information security controls such as access controls that only grant access and permissions on a need-to-know basis ("least-privilege") in section 4.2 of the Code.

B. Information security controls such as access reviews on a regular frequency in section 4.2 of the Code.

C. Information security controls such as data handling and disclosure procedures appropriate for the level of risk associated with the processing activity in section 2.6 and 4.2 of the Code.

D. Training and awareness for personnel authorised to process Personal Data that covers the confidentiality obligations related to the processing activity in section 2.4.o and 2.6 of the Code.

E. Contractual confidentiality clauses as per section 2.4.q and 2.6 of this Code.

Examples:

- CRO engaged in monitoring (see list of services in Appendix 2) ensures that the monitors sign employment contracts that include provisions on confidentiality obligations towards Personal Data of Study Subjects; scope of training records for monitors contain rules prohibiting retrieval of non-pseudonymised source records at the time of direct access to data.
- CRO providing medical monitoring, safety reporting, pharmacovigilance (see list of services in Appendix 2) may receive unintentionally from the Investigational Sites, improperly pseudonymised records. In this case the CRO must instruct a GDPR incident and all related documentation (e-mail correspondence, incident report and assessment forms …) must be filed.
- CRO providing IT-managed services, e.g., online electronic data capturing platform (see list of services in Appendix 2) shall incorporate into its IT product the appropriate security-preserving tools and features as early as possible within the product design and development, and continuously integrate and perform relevant tests.
- CRO delivering direct-to-patient services (see list of services in Appendix 2) shall organise the data processing with access and other applicable permissions being granted on the need-to-know basis, e.g., via segregation of the systems and databases used to process identifying Study Subjects' data for the direct-to-patient service and those purposed for the processing of pseudonymised health-related data used for other CRO services delivered to the sponsor.

3.6.1 Pseudonymisation

Pseudonymisation is used in Clinical Research in order to protect the privacy and rights of the Study Subjects[10]. By default, all data processed by CROs should be pseudonymous and identifying data should only be processed by exception and in accordance with section 3.6.3. In order to make datasets pseudonymous, a process is applied to replace the Study Subject's directly identifying Personal Data with a subject identification code. Pseudonymous datasets may include indirect identifiers but must exclude direct identifiers. Pseudonymous data is still Personal Data.

- Direct identifiers can be used to identify a person without additional information or by cross-linking with other information that is in the public domain.

  It is advisable to treat other individualised information such as medical record numbers and phone numbers as direct identifiers, even though additional information is required to link them to an identity, because these forms of identification are extensively used and thus available for linking to identities.

  Examples of direct identifiers are the following:

  Name, address, telephone number, e-mail addresses, and other unique identifying numbers, characteristics or codes like vehicle identification number, social security number, social insurance number, photographs of distinguishing features, and biometrics (as defined by the GDPR).

- Indirect identifiers are data that by themselves do not identify a specific individual but can be aggregated and linked with other information to identify data subjects.

  The subject identification code that may be used for pseudonymisation is an indirect identifier.

  Other examples of indirect identifiers include:

  Sex, date of birth or age, geographic locations (such as postal codes, census geography, information about proximity to known or unique landmarks), IP address, language spoken at home, ethnic origin, total years of schooling, marital status, criminal history, total income, visible minority status, profession, event dates, number of children, high level diagnoses and procedures.

Note:

If a CRO is providing a service to the data controller that involves generating subject identification codes, e.g., as part of the functionality of a CRO-operated IWRS system, the CRO should ensure that the codes exclude identifiers of the Study Subjects such as

[10] Article 29 Working Party's Opinion 5/2014 on Anonymisation Techniques or any subsequent version thereof

identification or insurance numbers, state/country numbers, initials, date of birth, or age. CRO should ensure that the codes are robust enough as a method of pseudonymisation and present a random sequence of symbols avoiding recognisable patterns within one Study that might pose a re-identification risk. CRO should take into consideration the risk of re-identification and shall ensure they choose the appropriate techniques to mitigate the risk identified.

Note:

Device numbers may, in certain use cases, constitute a "direct identifier". As such, they should be treated on a case-by-case approach, considering their usage and their related potential for/risk of re-identification.

3.6.1.a A CRO shall process Personal Data of Study Subjects only in pseudonymous form, unless processing of direct identifiers is strictly necessary for the provision of the services and is carried out upon instructions from the data controller in compliance with the principle of data minimisation.

Examples:

Due justification for a CRO to process direct identifiers may include the following cases:

- CRO is contracted by the Sponsor for the delivery of direct-to-patient services (see list of services in Appendix 2, class (8)) processes direct identifiers because fulfilment of the purpose is impossible without access to such data.
- CRO's monitors and internal auditors (see list of services in Appendix 2, classes (5), (15)) will have access to Study Subject identification logs/patient registry, including for verification of consenting process and consistency of CRF completion from source records.

3.6.2 Anonymisation

It may be desirable to process a dataset outside of the Research protocol, which may be possible under the condition that data are anonymised. The Opinion of the Art. 29 Working Party[11] which is referred to by the European Medicines Agency (EMA) guideline[12], and any updated version of these guidelines, set a high threshold for achieving anonymisation. Data shall be considered anonymised when it is rendered into a form which does not identify individuals and where identification through "*all the means likely reasonably to be used*" by either the controller or a third party, including combination of data with other data, is not likely to take place.

A CRO may offer anonymisation as a service. They shall document the anonymisation process and provide assistance to the data controller in setting the parameters and evaluating the re-identification risks on the resulting dataset.

Note:

CRO shall apply anonymisation methods that align with the recognised standards and/or are based on the guidance, recommendations of the European Data Protection Board, national data protection supervisory authorities, and supervisory authorities governing the domain of clinical research, e.g., EMA.

3.6.2.a A CRO providing anonymisation as a service shall have staff experienced in data analysis who can perform an analysis of re-identification risk in order to demonstrate to the Sponsor that a dataset is anonymous.

3.6.3 Processing both Directly and Indirectly Identifiable Personal Data of Study Subjects

Staff of the CRO may receive or access directly and indirectly identifying Personal Data of Study Subjects for the following purposes:

(1) Monitoring and ensuring reliability of Clinical Study Data through verifying that the Investigator transfers data from the medical records to CRFs precisely and accurately. CRO shall not transmit these data into its computer systems for further processing, so the relevant obligation of the CRO consists in complying with requirement 2.6.a and 2.6.b of this Code; however in cases where the CRO

[11] Article 29 Working Party's Opinion 05/2014 on Anonymisation Techniques (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf) or any subsequent version thereof

[12] EMA's External Guidance on implementation of Policy 0070 of 2019 (https://www.ema.europa.eu/en/documents/other/european-medicines-agency-policy-publication-clinical-data-medicinal-products-human-use_en.pdf)

shall process the Personal Data in its computer systems e.g., for remote source data verification, the additional provisions of this section 3.6.3 shall also apply.

(2) Providing supplementary services, which will require processing of the directly identifying Personal Data of the Study Subjects, e.g., name, postal address, electronic and telephone contact details, bank details, etc., with complete separation from pseudonymised data concerning Study Subjects' health.

Examples:

- A CRO provides transportation services, including special transport; travel arrangement, including plane, train, taxi, accommodation bookings.
- A CRO provides e-products allowing direct interaction with patient via online platforms or electronic messaging systems, including electronic patient recorded outcomes (ePRO) or permitting patients to be electronically consented for participation in the Study (eConsent), etc.
- A CRO provides assistance to the Sponsor in responding to data subjects' requests and rights.
- A CRO provides monitoring services to the Sponsor and has to view the source documents containing direct identifiers. Ordinarily when monitoring is performed, there shall not be a transmittal of identifiable personal data to the computer systems of the CRO, but in the cases where there is processing in the CRO's computer systems of identifiable Personal Data for remote source data verification purposes, the CRO must refer to and comply with all applicable European and national guidelines on remote monitoring such as the Recommendation paper on decentralised elements in clinical trials by EMA, Version 01, 13 December 2022.
- Representatives of patient advocacy groups/organisations communicate face-to-face with Study Subjects and their families to understand, share information with the clinical research community/stakeholders, and address the concerns and difficulties that the Study Subjects experience during their participation in a Study.

3.6.3.a A CRO shall have the processes in place enabling the CRO to assist the controller to define the minimum Personal Data of Study Subjects necessary for the CRO to provide the services that require CRO's access to both the direct identifiers and pseudonymised data of Study Subjects.

3.6.3.b Where processing directly identifiable Personal Data, CRO shall implement appropriate higher technical and organisational security measures as per applicable European and national guidelines[13] to ensure that the confidentiality of Personal Data of Study Subjects is maintained.

Notes on higher technical and organisational measures:

- The CRO can outsource the processing of direct identifiers to a sub-processor that will have direct interaction with Study Subjects. CRO should receive accountability documents from these vendors. CRO shall ensure that evidence of service delivery e.g., invoices, do not capture direct identifiers of Study Subjects that can increase the risk of reversing the pseudonymisation.
- CROs that process the direct identifiers themselves as well as the pseudonymous data shall apply additional technical and organisational measures consisting of higher standards of data segregation, access control, and transparency about the processing. Measures are aimed to prevent combination of directly identifying and pseudonymised data and the associated risks of inadvertent reversal of pseudonymisation[14].

  Such measures shall be aimed to ensure the following:

  1) Segregation between the systems and databases used to process directly identifying Personal Data and pseudonymous data sets via:
     - Access control of the locations, systems and databases containing directly identifying Study Subject data so that the data are not inadvertently exposed to unauthorised personnel.
     - Staff control, namely preventing staff engaged to process directly identifying from being engaged in delivering the services using pseudonymous data and vice versa.
     - Preventing staff from combining information from different sources to associate individuals with the Study, e.g., involving only minimal number of staff or contractors to process directly identifying data of Study Subjects; staff

[13] Recommendation paper on decentralised elements in clinical trials by EMA, Version 01, 13 December 2022

[14] Article 29 Working Party's Opinion 5/2014 on Anonymisation Techniques or any subsequent version thereof

assigned to process identifying data of Study Subjects will not be a member of a project team assigned to oversee the Clinical Study.

- Communication control, namely via the Investigational Site and not with the patients directly whenever possible, and when services require direct communication with Study Subjects the CRO shall minimise data collection and use tokenised IDs for the Study Subjects wherever possible.
- Contractual control, namely including dedicated provisions in confidentiality agreement with the assigned staff; provisions specifying the permitted disclosures.

2) The CRO provides enough information about the methods of processing to the Sponsor where the CRO shall be processing both directly identifying and pseudonymous data so that the Sponsor can ensure that Study Subjects are fully informed in advance of the terms of data processing as required under the applicable data protection law.

3) The CRO has appropriate processes and documents in place to demonstrate accountability for their implementation, including records of processing, specific to the completion of these tasks. All such documents shall be revised in a timely fashion and securely maintained.

4 Obligations of the CRO as processor

The Sponsor relies upon the CRO to fulfil its obligations as a processor to ensure the lawful and fair processing of Personal Data. This ensures that the rights and freedoms of data subjects are maintained.

Key obligations of the CRO are (as applicable):

- Designation of a Data Protection Officer
- Administration of appropriate technical and organisational measures (TOMs)
- Maintenance of required data processing records
- Management and audit of sub-processors
- Assistance to, and collaboration with, controllers
- Data transfers to Third Countries

Application domain: Requirements explained in each section of this chapter apply generally, i.e., to all classes of services listed in Appendix 2, except classes (1) and (2).

4.1 Designation of a DPO

Article 37 GDPR: a DPO designation shall occur when *"the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and Personal Data relating to criminal convictions and offences referred to in Article 10."*

A Data Protection Officer (DPO) shall be designated by the CRO where it is required under the GDPR. Given that CROs, regardless of the number of employees and CRO's size, process health data, which is a special category of Personal Data, mostly on a large scale it is highly likely a DPO shall need to be designated by the CRO.

Example:

- A CRO that only has a small number of employees shall likely need to designate an external DPO in order to avoid the conflict of interests between an operational role and the DPO position.

A CRO might also be required to designate a DPO when "*regular and systematic monitoring of data subjects on a large scale*" is occurring, for example where there are wearable devices being used in the Study that monitor the health status of Study Subjects. CROs shall follow the guidance provided by the relevant data protection authority and European Data Protection Board guidelines to determine whether they should appoint a DPO.

It is important to note that it is the CRO's decision to determine whether a DPO is required. Regardless of the applicability of the mandatory designation, CROs are encouraged to designate a DPO on a voluntary basis. The Sponsor's feedback can be considered, but it shall not be the determining factor. In case a CRO estimates that it does not need a DPO and duly motivates such a choice of not designating one, other mechanisms for ensuring compliance to the GDPR should be adopted. The functions normally performed by the DPO should be provided for internally despite the lack of a DPO; for instance, internal processes should be established so that processing activities are duly monitored and registered, risk assessments are carried out when needed, a contact point is identified to assist with data subject requests and rights, proper training on GDPR compliance is provided to employees, a contact point is identified for liaising with supervisory authorities, etc.

A CRO's DPO shall not also act as the Sponsor's DPO given the possible conflict of interest.

Example:

- The data controller's DPO has an obligation to monitor compliance of the data processing by the data processor. If the CRO's DPO acts as the DPO of the Sponsor (controller), that DPO would be monitoring the data processing of both Sponsor and CRO (processor). The DPO may face a challenge when monitoring data processing of the CRO upon detecting a non-compliance from the CRO. The DPO would be placed in position where their objectivity is questionable, and they may find it difficult to act in the Sponsor's interests where that may require acting to the detriment of the CRO that employs the DPO.

4.1.a CRO shall designate a DPO for the organisation if the requirement in Article 37 GDPR is fulfilled. If a DPO is not designated, CRO shall document the reasons why a DPO was not designated and what support is provided in place of a DPO to comply with the GDPR.

4.1.b CRO shall appoint a DPO based on their qualifications and ability to carry out the tasks under the GDPR. The CRO shall not interfere with the DPO's carrying out of their tasks under the GDPR.

4.1.c CRO shall support the DPO in the carrying out of their tasks by providing resources to carry out those tasks and involve the DPO in a timely manner for matters involving data protection.

4.1.d CRO shall have the DPO report to senior management within their organisation.

4.1.e CRO shall ensure that the contact information of the DPO is included in the records of processing and made readily available through their privacy notice within their organisation, to concerned data subjects, and to the Sponsors and supervisory authorities as needed.

4.2 Technical and Organisational Measures (TOMs)

This section specifies the requirements for the implementation of the technical and organisational measures to ensure and to be able to demonstrate, that processing is performed in accordance with Article 32 GDPR "Security of processing";

> *"[…] the controller and the processor shall implement **appropriate technical and organisational measures** to ensure a level of **security appropriate to the risk** […]*
>
> ***Adherence to an approved code of conduct** […] or an approved certification mechanism […] may be used as an element by which to demonstrate compliance with the requirements set out in […] this Article."*

In accordance with the GDPR requirements, both the controller and the processor (and thus the CROs) shall implement organisational and technical measures to ensure appropriate level of security with regards to the risks associated with the data being processed.

An Information Security Management System (ISMS) is a systematic approach consisting of processes, technology and people that helps protect and manage an organisation's information through effective risk management. An ISMS contributes to compliance with the Article 32 GDPR requirements for a CRO to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. However, the implementation of an ISMS alone does not constitute compliance with Article 32 GDPR. The CRO achieves compliance by implementing all the applicable measures from the Code as defined in their Code Statement of Applicability (see section 1.10 of the Code).

Security measures shall be selected according to the state of the art balanced with the costs of implementation. Measures shall consider the context of processing; the nature of the data being processed and the scope of the processing. The likelihood of the risk and the severity to the rights and freedom of the data subjects shall be considered to select appropriate organisational and technical measures. A CRO adherent to this Code of Conduct must have an operational Information Security Management System (ISMS) compliant with the requirements specified and listed in document 02 of the Code, whose title is "Security Objectives and Requirements".

Note:

- Most CROs have a Quality Management System (QMS) and, very frequently this QMS is part of an ISO 9001 certification. In a number of cases, complementing the QMS with appropriate information security measures may be sufficient to obtain an ISMS enabling adherence to the Code.

The requirements specified in document 02 are controls that have been derived from the following existing standards:

1. ISO/IEC 27001: May 2017[15], Information technology – Security techniques – Information security management systems – Requirements;
2. ISO/IEC 27701: August 2018, Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines.

For all classes of services, **certification on the ISO 27001 standard is not required** but constitutes a favourable condition for adherence.

Application domain: Requirements in this section apply to all classes of services listed in Appendix 2, and as further elaborated and specified in document 02 of the Code.

4.2.a The CRO shall establish, implement, maintain, and continuously improve an Information Security Management System aligned with the methodology exemplified by ISO27001 or any equivalent compliance framework. This means that the CRO shall:

- Implement a risk analysis methodology in order to evaluate the risks;
- Implement security policies;
- Implement security controls to reduce the identified risk;
- Assess the performance of each control being set up; and
- Ensure corrective and preventive action in order to improve the performance of the security measures.

The scope of applicability of the ISMS shall clearly be identified. Each item outside the scope of applicability must clearly be documented.

4.2.b A CRO adhering to this Code shall implement the control requirements listed in Document 02 of this Code that apply to the classes of service that the CRO lists in their Statement of Applicability.

4.2.c All ISMS documents shall be versioned and mechanisms to retain obsolete versions shall be documented.

4.2.d The requirements derived from the Statement of Applicability of the CRO that concern information security, shall all be covered by the ISMS of that same CRO.

To ensure compliance to the security requirements of the Code, the CRO must pursue several security objectives which must be detailed in the organisation's ISMS that must be consistent with the Statement of Applicability of the CRO.

Any exclusion of a specific control from the ISMS must duly be documented and justified with regards to the services offered by the CRO.

4.2.e Any exclusion of a control requirement derived from the Statement of Applicability shall be listed and justified.

4.3 Records of processing activities

The CRO must maintain records of processing activities as outlined in Article 30 of the GDPR. CROs often use applications and tools dedicated to Research, Studies and evaluation. Sponsors may also rely on these application tools and for maintaining their own records. CROs must be able to demonstrate availability of such processing records relevant to the services provided by the CRO.

[15] For the avoidance of doubt, ISO 27001:2022 is compatible with this Code and the requirements can be read accordingly.

It is important to note that the CRO's records are not the same requirements as those for a Sponsor's role as a data controller. The Code refers to records that are limited to processing activities carried out as a processor on behalf of the Sponsor (controller). CRO's data processing records are separate from those required of the Sponsor (controller).

Application domain: Requirements explained in each section of this chapter apply generally, i.e., to all classes of services listed in Appendix 2, except classes (1) and (2).

4.3.a The CRO shall maintain a record of processing activities within the span of its control. CRO is free to define the format as long as the report includes the elements defined under Article 30(2).

4.3.b The CRO shall establish jointly with the controller the process to provide the records of processing to the supervisory authority upon request without undue delay.

4.4 Management & audit of sub-processors

Where the CRO enters into the contractual agreement with vendors who are engaged as sub-processors, those contracts are subject to section 2.4, 2.5, 2.6 and 2.7 of this Code of Conduct. For vendors contracted directly by the CRO, the CRO is responsible for ensuring that such sub-processors utilised to process Personal Data for the Sponsor implement the appropriate technical and organisational measures to keep Personal Data secured and act in accordance with the Sponsor's instructions. The CRO is responsible for the performance of sub-processors engaged as defined under Article 28(4) GDPR.

The Sponsor (controller) will generally delegate the CRO to select the appropriate sub-processors. While the Sponsor may delegate the selection and engagement of vendors as sub-processors, the CRO shall engage such sub-processors in compliance with section 2.5 of this Code of Conduct, and keep the Sponsor engaged as appropriate throughout this process. The selection process must take into consideration the competence and compliance capabilities of the sub-processor namely their ability and commitment to provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing of Personal Data entrusted to them will meet the requirements of the GDPR..

Application domain: Requirements explained in each section of this chapter apply generally, i.e., to all classes of services listed in Appendix 2, except classes (1) and (2).

4.4.a The CRO shall have written procedures for approving, managing, and removing sub-processors.

4.4.b When selecting sub-processors, a CRO shall use its expertise to conduct a selection process that will ensure that the CRO selects only the sub-processors that will be able to provide the same technical and organisational measures that the CRO is bound to provide in the Data Processing Agreement.

4.4.c Where the CRO performs their due diligence and monitoring through an audit of the sub-processors, the audit shall be performed by a qualified and experienced auditor that follows a defined privacy audit plan.

4.4.d The CRO shall regularly monitor compliance with and the effectiveness of the sub-processor's technical and organisational measures.

4.4.e The CRO shall report any significant and unresolved non-compliance issues with a sub-processor to the data controller.

Example

- A CRO was directed by a Sponsor to engage a specific vendor as a sub-processor. The CRO, not the Sponsor, will hold the contractual relationship with the sub-processor. During the course of negotiations, the sub-processor refuses to incorporate the same TOMs as the Sponsor has imposed on the CRO.

  The Sponsor directs the CRO to accommodate the sub-processor's preferences for the TOMs. The CRO audits the sub-processor to determine that the sub-processor's TOMs are going to provide the same levels of data protection as the TOMs in the CRO's contract with the Sponsor.

4.5 Assistance to, and collaboration with controllers

Application domain: Requirements explained in each section of this chapter apply generally, i.e., to all classes of services listed in Appendix 2, except classes (1) and (2).

4.5.1 Provision of advice on Clinical Research data protection matters to a Sponsor

A CRO may provide advice on Clinical Research data protection matters to a Sponsor but shall not be, at any time, in a position of decision making on such matters.

However, if the CRO deems that the Sponsor (controller) is not aligned with the GDPR, the CRO shall inform the Sponsor immediately and can provide guidance on what in its opinion, would bring the Sponsor (controller) into alignment with the GDPR.

4.5.1.a The CRO shall inform the Sponsor if, in CRO's opinion, an instruction from the Sponsor infringes the GDPR or other Union or Member State data protection provisions.

The CRO can share insights and observations but the Sponsor should rely upon their own DPO or privacy subject matter expert for final determination regarding their response to CRO's notification.

4.5.2 CRO as a representative of a Sponsor as a controller under Article 27

Article 27 of the GDPR applies when a controller (Sponsor) is not established in the European Union when the processing of Personal Data of data subjects in the EU is taking place. Often in Clinical Research the Sponsor/controller does not have either legal or physical presence within the EU. However, when defining the applicability of Article 27 GDPR, it should be noted that the determining factor is not the legal form of company arrangements i.e., whether the company has constituted a legal branch or subsidiary, but rather that an establishment implies the effective and real exercise of activity through stable arrangements, as per recital 22 of the GDPR. There may be circumstances where the Sponsor requests that the CRO act as its representative. Pursuant to the opinion expressed by the European Data Protection Board in the guidance about the territorial applicability of the GDPR[16], a CRO shall not act as a processor and Representative for the same Sponsor, due to a possible conflict of obligation and interest that may arise in case of enforcement proceedings. This does not prevent a CRO taking on the role of representative for a Sponsor for which it does not act as processor.

[16] EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1 12 November 2019

4.5.2.a A CRO shall only act as an EU data protection representative of a Sponsor under condition that the CRO does not at the same time act as a data processor for any Clinical Research of this Sponsor.

4.5.3 Data protection impact assessment

The Sponsor, as data controller, is also obliged to perform a data protection impact assessment on any envisaged processing operations of Personal Data that may be likely to result in a high risk to the rights and freedoms of natural persons. CRO, as data processor, is not obliged to have undertaken such an assessment itself on the processing activities it performs but is obliged to assist the Sponsor in the undertaking of Sponsor's assessment.

4.5.3.a CRO shall, upon Sponsor's request, assist the Sponsor in completing a data protection impact assessment within the limits of the services that the CRO provides under the Service Contract and the related Data Processing Agreement.

4.5.4 Data subject requests

Both the Sponsor and CRO work with pseudonymised data concerning health of Study Subjects and identifiable Personal Data of Healthcare Professionals. When responding to a data subject request from a Healthcare Professional, CRO shall ensure that it has processes in place to fulfil the obligations elaborated in the Data Processing Agreement as per requirement 2.4.g of this Code.

While pseudonymised data is still Personal Data, it is not directly attributable to a specific data subject. Study Investigational Sites may be the primary area where data subject requests can be exercised. To the extent that it is not incompatible with the CRO only processing pseudonymous data, the CRO must provide support to the Sponsor in responding to the data subject requests e.g., by helping to facilitate the exercising of these rights by relaying the instructions of the Sponsor to the Study site. The CRO may be asked to produce evidence of a process to execute data subject requests in a timely manner. This evidence may take the form of description of processes, procedures and other documentation that captures metrics, key performance indicators and monitoring.

4.5.4.a A CRO, in agreement with the Sponsor, shall establish and document a process to carry out communication with the Sponsor for the purpose of providing assistance to the Sponsor with responding to data subjects' requests in case a Study Subject contacts the CRO directly.

Examples:

- Study Subjects should always be enabled to contact the data controller directly. However, since the Sponsor and CRO shall normally not receive identifying data of the Study Subjects in order to preserve confidentiality of their participation and (potentially) blinded nature of the Study, the CRO may propose to the Sponsor to arrange that the Study Subjects are invited to address requests to the Healthcare Professional who will facilitate the execution of their data subjects' rights. The right for the Study Subject to contact the Sponsor directly should always be reserved regardless of other arrangements.

  As a rule, such recommendation will be communicated to the Study Subjects via Informed Consent Form or a separate notice. The Healthcare Professional shall be instructed to notify the CRO or/and Sponsor of a data subject request and seek instructions from the Sponsor/CRO on how to handle the request.

- Unless the CRO is performing a direct-to-patient service (see list of services in Appendix 2, class (8)), normally Study Subjects will not be provided with data processors' contact details for the exercise of data subject requests. However, if the CRO and Sponsor arrange otherwise, CRO shall ensure that identifying data of the Study Subjects making a data subject request, such as full name, e-mail address, etc., and their pseudonymised data concerning health shall not be combined in their data processing systems. This can be done via appointing different teams to handle data subject requests from the Study Subjects and to process Study Subjects' pseudonymised health-related data collected for the primary research purposes. However, in cases where the CRO receives a data subject request, the CRO shall ensure it is able to attribute the request to the correct data subject by combining identifiers and the health data in a punctual manner. Once the exercise of rights has been completed, the CRO shall remove the directly identifying data of the Study Subject from its databases, while retaining records to evidence compliance with the request e.g., by redacting or hashing direct identifiers.

In case a CRO delivers to the Sponsor a direct-to-patient service (see list of services in Appendix 2, class (8)), Study Subjects are entitled and may with high probability contact the CRO with a request to execute their data protection rights, i.e., data subject request, or with other enquiries. In such case the CRO shall implement special security arrangements as provided in section 3.6.3 of this Code.

4.5.5 Personal Data Breaches

According to Article 4(12) of GDPR, 'Personal Data Breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

This refers to any incident of security, whether malicious or not and occurring intentionally or unintentionally, that has the effect of compromising the integrity, confidentiality or availability of Personal Data.

The notification of a Personal Data Breach is not required in all circumstances:

- Notification to the competent supervisory authority is required unless a breach is unlikely to result in a risk to the rights and freedoms of individuals.
- Communication of a breach to the individual is only triggered where it is likely to result in a high risk to their rights and freedoms.

The controller bears the responsibility for the protection of Personal Data. This includes the responsibility to seek to contain the incident, to assess the risk that could result from it, and determine whether it is required, to notify the Personal Data Breach with the supervisory authority as well as to communicate the Personal Data Breach to the data subject.

Note:

- It has to be noted that a CRO could make a notification to the supervisory authority on behalf of the controller, if the controller instructed the CRO to make notifications on its behalf and this is part of the contractual arrangements between CRO and controller. However, it is important to note that the legal responsibility to notify remains with the controller.

The CRO, for its part, as a data processor, must assist the controller in ensuring compliance with its obligations.

Regarding Personal Data Breaches, the assistance provided by the CRO shall consist in particular of:

- notifying the controller "without undue delay" when it becomes aware of a Personal Data Breach without firstly assessing the likelihood of risk arising from the Personal Data Breach; it is the controller that must make this assessment on becoming aware of the breach;
- more generally in reporting all information the CRO has access to which are necessary to enable the controller to comply with its obligations. This reporting can be made in phases as more details become available; and
- in assisting the controller to take appropriate remedial action to address the Personal Data Breach.

Note:

- Where the CRO provides services to multiple controllers that are all affected by the same incident, the CRO will have to report details of the incident to each controller.

The practicalities of the assistance provided by the CRO to the controller shall be described within the Data Processing Agreement which has to clarify the responsibilities of the parties.

4.5.5.a CRO shall have appropriate technical and organisational measures in place to ensure an appropriate level of security of Personal Data; the ability to detect, address, and report a Personal Data Breach to the controller in a timely manner shall be seen as essential elements of these measures.

For example, to detect a Personal Data Breach a CRO could use certain technical measures such as data flow and log analysers, from which is possible to define events and alerts by correlating any log data.

4.5.5.b CRO shall implement a documented notification procedure in place, setting out the notification process to be followed by the CRO's employees and all others

professionals who intervene in the Clinical Research when they face a security-related event to assist them to notify these information concerning security-related events to the CRO's responsible person (e.g., the CRO's DPO) or CRO's persons with the task of addressing incidents, in order to establish the existence of a Personal Data Breach.

4.5.5.c CRO shall implement training to teach employees and all other professionals who intervene into the Clinical Research how to react to security-related events including Personal Data Breaches and to respect CRO's procedures and mechanisms in place.

4.5.5.d CRO shall establish an internal register of Personal Data Breaches in order to document the Personal Data Breach they face regardless of whether it is a Personal Data Breach required to be notified or not; this internal register shall contain (i) the same key information which has to be included within the internal register kept by the controller as required by Article 33(5) to assist the controller to document its own register of Personal Data Breach (ii) the records of the actions taken by the CRO to assist the controller to comply with its obligations.

4.5.5.e CRO shall have a documented notification procedure[17] to submit to the agreement of the controller when they enter into a contractual relationship setting out the process to follow to assist the controller in a timely manner when a Personal Data Breach occurs including for example (i) effective communication channels (ii) notifications deadlines (iii) person in charge.

4.5.5.f When a CRO has appointed a DPO, the DPO shall be promptly informed about the existence of the Personal Data Breach and involved throughout the breach management and notification process. Otherwise, a person in charge, possessing the necessary competence and knowledge of data protection arising from appropriate training, must be appointed to deal with these issues and to be in contact with the controller.

Example:

- In the course of safety reporting, an Investigational Site sends to the CRO copies of medical records of a Study Subject for the assessment of the adverse event. The CRO's safety team detected that the copies of medical records contain the unredacted full name of the Study Subject which would make it possible to re-identify the Study Subject.
  - The CRO's employee trained to identify a Personal Data Breach, promptly informs the DPO and/or other responsible representative of the CRO, as applicable, using the communication channel identified in the CRO's internal procedure.
  - The DPO and/or other responsible representative of the CRO, as applicable, promptly informs the DPO and/or other responsible representative of the controller using the communication channel and the forms to document the Personal Data Breach identified in the notification procedure already agreed with the controller.
  - The CRO ensures that this Personal Data Breach is contained and under control. Otherwise, the CRO reports documented information in phases as more details become available.
  - The CRO remains at the disposal of the controller to assist him to comply with his obligations and asks for his instructions before undertaken any action regarding the Personal Data Breach.
  - The CRO formally reminds the Investigational Site of its obligations under the GDPR.
  - The CRO records the Personal Data Breach in its own internal register of Personal Data Breach.

4.6 Data transfers to Third Countries

For the avoidance of doubt, the Code of Conduct in its present form is not intended to be a Code of Conduct as a tool for international transfers per Article 46(2)(e) of the GDPR. A CRO adhering to the Code of Conduct

[17] EDPB Guidelines 9/2022 on Personal Data breach notification under GDPR

should inform the controller thereof and explain that adherence of a CRO to the Code cannot replace such legal transfer tools.

Application domain: Requirements explained in each section of this chapter apply generally, i.e., to all classes of services listed in Appendix 2, except classes (1) and (2).

International transfers of Personal Data falling within the scope of this section comprise transfers of Personal Data made in the context of any of the services covered by this Code and are subject to Article 44 GDPR;

> "*Any transfer of Personal Data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation,* ***the conditions laid down in" the Chapter V of the GDPR "are complied with by the controller and processor*** *[…]'.*

4.6.a The CRO shall ensure that for each case of international transfer of Personal Data performed in the course of providing its services, the following is listed in the Data Processing Agreement:

1. A description of the transfer, including the legal basis for the transfer and the location of the Importer and the assessment of the applicable legislation to the Importer to the specific transfers where there is no applicable adequacy decision and where the transfers are not based on derogations;
2. Under the instructions from the Sponsor, the selected transfer tool on the basis of which the transfer is allowed by the GDPR, namely (a) adequacy decision in force by the European Commission; (b) an agreement based on the standard contractual clauses adopted by the European Commission; (c) appropriate binding corporate rules; (d) a Code of Conduct applicable to the domain of scientific research with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; (e) an approved certification mechanism pursuant to Article 42 of the GDPR; or (f) *ad hoc* contractual clauses under Article 46(3)(a) of the GDPR; or (g) one of the Article 49 derogations[18], including consent of the data subjects, when specific conditions may legitimate such international transfer; and
3. Any other instructions from the Sponsor relating to transfers of Personal Data, including any supplementary measures[19] required to be adopted, if applicable.

Example:

- A CRO adhering to the Code will implement controls applicable for their services as per document 02 and may propose to the Sponsor that such controls be approved by the Sponsor as fulfilling the requirement for adequate "supplementary measures".

4.6.b The CRO shall provide information to the Sponsor on which transfer tool it intends to use, based on the results of its transfer impact assessment[20] and on the adopted safeguards to address any remaining risks associated within international transfers.

4.6.c The CRO shall communicate to its sub-processors to whom data are transferred the data controller's instructions regarding the transfer of Personal Data to Third Countries. The CRO may provide additional instructions to such sub-processors

[18] EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 679/2016

[19] EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, adopted on 18 June 2021

[20] EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, adopted on 18 June 2021

provided that these additional instructions do not conflict with the instructions of the data controller.

4.6.1 CRO as Exporter

This section specifies the requirements for the CRO when the CRO is acting as an Exporter on behalf of the controller involved in the transfer of Personal Data outside of the European Union, in accordance with chapter V GDPR and the recommendations of the European Data Protection Board[21] post the decision in C-311/18 - Facebook Ireland and Schrems. Therefore, CROs acting as Exporters, where appropriate together with the Importer, need to determine on a case-by-case basis and taking into account the circumstances of the transfer whether or not the law or practice in the Third Country destination prevents from complying with the level of protection essentially equivalent to the one in the EU and, where necessary, supplement the selected transfer tool with any appropriate additional measures. Considering that the transfer is a processing activity carried out on the behalf of the Sponsor (data controller), the CRO shall remind the Sponsor that they could also be responsible and could be liable under Chapter V GDPR for transfers performed by CRO[22].

If CROs acting as Exporter are unable to take appropriate supplementary measures to guarantee an essentially equivalent level of protection under EU law, they are required to suspend or end the transfer of Personal Data.

This section covers the scenario where there is either:

a. A CRO seated in the EU transferring Personal Data to sub-processors seated in a Third Country (otherwise known as a “processor to processor” transfer); or

b. A CRO seated in a Third Country transferring Personal Data to sub-processors also seated in a Third Country when the transfer concerns Personal Data of data subjects participating in a Clinical Study who are in the EU (otherwise known as a “processor to processor transfer”).

c. A CRO seated in the EU transferring Personal Data to a Sponsor seated in a Third Country (otherwise known as a “processor to controller” transfer); or

d. A CRO seated in a Third Country transferring Personal Data to a Sponsor also seated in a Third Country when the transfer concerns Personal Data of data subjects participating in a Clinical Study who are in the EU (otherwise known as a “processor to controller transfer”).

Examples:

- A global CRO performing start up services exports Investigator Personal Data from its EU entities to a sub-processor hosting data in the non-EU countries (scenario a).
- A CRO hosting an EDC system exports Personal Data by replicating data from its EU data centre to its back up data centre in the non-EU countries (scenario a).
- A CRO providing eTMF services in one non-EU country exports Personal Data to another CRO seated in a different non-EU country (scenario b).
- A CRO in an EU country performing pharmacovigilance services provides Personal Data received as serious adverse events to a Sponsor’s medical team in a non-EU country (scenario c).
- A CRO based in a non-EU country providing medical monitoring services transfers Personal Data of data subjects at EU Investigational Sites to a non-EU based Sponsor (scenario d).

Distinction must be made between the CRO who is acting as an Exporter under its own internal processes to provide its services within the framework of the Service Contract and a CRO who is acting as Exporter under the direction of a Sponsor located outside EU. This scenario may occur when the CRO who is acting as an Exporter to provide its services within the framework of the Service Contract needs to transfer Personal Data due to its internal processes rather than at the request of the Sponsor.

[21] EDPB Recommendation 1/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of Personal Data, and EDPB Recommendation 2/2020 on the European Essential Guarantees for surveillance measures.

[22] Section 19 of the EDPB Guideline 5/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.

Example:

The CRO needs to transfer Sponsor's data to Third Countries:

- To its subsidiaries in the Third Countries because the CRO staff who are engaged to process data in the context of the services are the employees of the concerned CRO subsidiary; or
- To a vendor of IT communication services established in a Third Country because that sub-processor provides the CRO with its corporate online platforms for video and audio conferences used in Investigator meetings and remote Investigational Site monitoring visits.

The CRO should make the Sponsor aware of such data transfers and comply with the authorisation requirements pursuant to paragraph 2 of Article 28 of the GDPR.

4.6.1.a The CRO who delivers the services to the Sponsor and acts as an Exporter under its own internal processes for the purpose of these services shall provide to the Sponsor a list of the locations of its data processing, in the manner agreed with the Sponsor in the Data Processing Agreement, and evidence that the provisions of Chapter V are complied with for the transfer according to the instructions of the controller, including that an appropriate transfer tool is used.

Example:

- CRO will list the Sponsor all CRO's affiliates that are engaged into processing for the concerned service, as well as all the vendors acting as sub-processors of the CRO, if this applies. CRO may agree with the Sponsor that the CRO provides access to a web-portal or similar, where the information on the processing locations is available for the Sponsor; or may include such lists of processing locations into the Data Processing Agreement.

4.6.1.b Any CRO who acts as an Exporter, whether under its own internal processes or under the direction of the Sponsor, shall keep records of international transfers of Personal Data that the CRO performs for such Sponsor, including the legal basis under Chapter V for each transfer.

Example:

- CRO may store the records of transfer as part of records of processing activities that a CRO shall maintain to comply with Article 30(2) GDPR. Records of transfer shall, if feasible and/or if Sponsor instructs the CRO to do so, in addition to the country of transfer/destination, indicate the type or/and name of processors in the destination country.

4.6.2 CRO as Importer

This section specifies the requirements for the CRO when the CRO is acting as an Importer in receipt of Personal Data that has been transferred outside of the European Union by another Exporter.

This section covers the scenario where there is either:

e. A CRO seated in a Third Country receiving Personal Data from a Sponsor seated in the EU (otherwise known as a "controller to processor" transfer); or

f. A CRO seated in a Third Country receiving Personal Data from another CRO or other data processor seated in the EU (otherwise known as a "processor to processor" transfer).

Examples:

- A CRO based in a non-EU country providing statistical analysis on a data set containing Personal Data of data subjects at EU Investigational Sites received from an EU-based Sponsor (scenario e).
- A CRO providing pharmacovigilance services hosted in the United States receives data exported by the Investigational Site on behalf of the Sponsor (scenario f).

4.6.2.a The CRO who delivers the services to the Sponsor and acts as an Importer for the purpose of these services shall provide to the Sponsor a list of the locations of its data processing and evidence that the provisions of Chapter V are complied with for the

transfer according to the instructions of the controller, including that an appropriate transfer tool is used.

4.6.2.b Any CRO who acts as an Importer shall provide the controller and Exporter with assistance on meeting the controller and Exporter's legal obligations including:

1. keeping controller and Exporter informed of any law or practice that prevents CRO acting as processor and Importer from maintaining the level of data protection essentially equivalent to the one in the EU;
2. making available all information needed by the controller and Exporter to assess the impact of the transfer to the Importer; and
3. having a policy to assess and implement supplementary measures in accordance with the instructions of the controller.

Example:

- CRO shall indicate any relevant law of the destination country it is aware of that may present a risk to the security and privacy of the Personal Data.

4.6.3 Transfers or disclosures not authorised by Union law

In line with Article 48 GDPR, a Third-Country request to transfer or disclose Personal Data does not, as such, make a transfer or disclosure lawful under GDPR. A request from a Third-Country court or from an authority does not in itself constitute a legal ground for such transfer or disclosure. A judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose Personal Data can only be recognised or enforceable if based on an international agreement such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to Chapter V GDPR.

In the absence of a framework provided by an international agreement or by another legal basis under the GDPR together with a ground for transfer, pursuant to Chapter V GDPR, CROs subject to EU law cannot legally base the disclosure and transfer of Personal Data on this type of request.

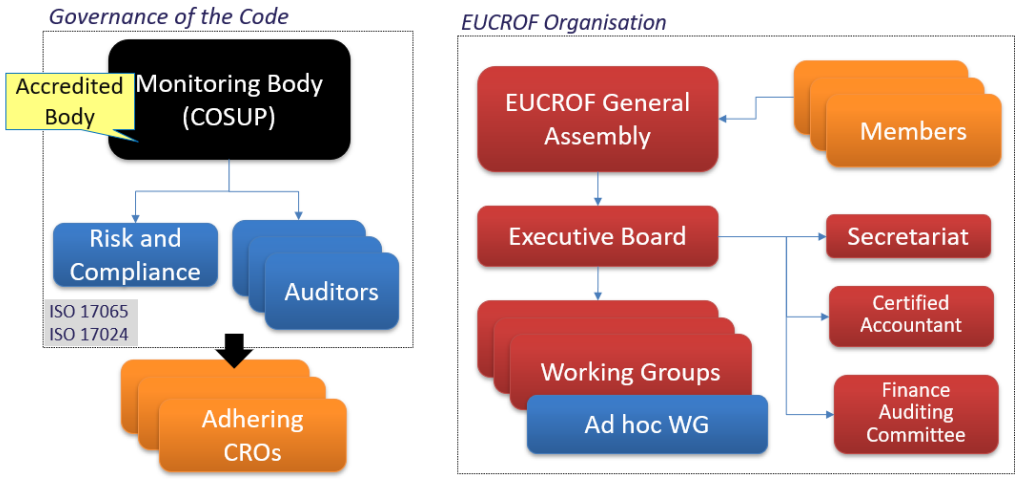
5 Monitoring and Compliance

5.1 Governance of the Code

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 of the 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*" as defined in section 1.4 (5) of this Code.

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



The scheme above outlines the organisation of the governance of the Code as an internal structure (left frame), independent of the decision making and executive bodies of EUCROF (right frame).

The COSUP is the body accredited by the competent supervisory authority in accordance with the officially established process before the Code of Conduct went into force. The COSUP delegates some of its tasks to the Risk and Compliance Officer who also performs regular internal audits, and recruits Auditors to audit candidates having selected to seek to obtain a Level 2 EUCROF Code Compliance Mark based on on-site audits. The *ad hoc* working group is a temporary working group which only purpose is to identify and propose candidates for the COSUP and document such candidacies.

5.1.1 Independence and impartiality

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*".

As regards impartiality, it is assured by:

- COSUP's Impartiality and Anti-bribery policy;
- the procedures relevant to auditing and remote auditing, which specify, among other, the way of selecting and supervise Auditors, in order to avoid conflicts of interest and, respectively, risks of bribery; and
- the procedure ruling COSUP decision-making, which specifies, among other, the measures to prevent its Members and the Auditors from being influenced.

To cover its operating expenses, COSUP invoices to the Code adherents, initial and yearly adherence fees. In addition, EUCROF, as Code Owner, allocates to the COSUP as necessary, an annual subsidy aimed at supplementing this source of income and guaranteeing the financing of the proper functioning of the COSUP.

For this purpose, the COSUP prepares an annual provisional budget with an income and expense statement. Provisional budget for year N is presented by it's President for approval by EUCROF General Assembly at the end or year N-1. The management of this budget is then placed under the exclusive responsibility of the COSUP without any interference or instructions of the Code owner. The COSUP will have its own bank accounts and payment means and will have full capacity to invoice.

The Human Resources procedure and the Governance and Quality Manual, ensure that COSUP has staff and management structures, accountability and function, separate from EUCROF and evaluates the performance of its auditors. The aforementioned auditing and decision-making procedures shall ensure that there are organisational and informational barriers and separate management structures for the Code Owner and the COSUP and that the latter acts free from instructions coming from EUCROF.

5.1.2 Legal Responsibility and Liability

The COSUP has the appropriate standing to carry out its role under Article 41(4) GDPR and is the body responsible for decision-making in accordance with section 5 of this Code. Nevertheless, as an internal body, the COSUP does not have autonomous legal standing to be held liable for the performance of its tasks and duties, under Article 83(4) GDPR. As such, pursuant to Article 83(4)(c) of the GDPR "*General conditions for imposing administrative fines*" and considering that (a) EUCROF is the owner of this Code and, (b) the COSUP is an internal body, EUCROF 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. Regardless, the monitoring body (COSUP) remains responsible to the supervisory authority for all tasks and decisions relating to its duties and the code owner shall take the necessary steps to ensure this.

5.2 The Supervisory Committee (COSUP)

5.2.1 Composition

The COSUP shall be composed of a maximum of 12 Members unless a larger number is decided by the General Assembly of EUCROF.

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.

Composition of the COSUP shall ensure that all these main domains of expertise will be represented in the COSUP and therefore the COSUP will, mandatorily have representatives with the requisite experience in data protection matters. In addition, all members of the COSUP will be required to have undertaken training in Data Protection and on the Code itself.

Membership of the COSUP shall reflect a balanced representation of stakeholders interested in the Code and shall even out the number of Members from each category, and this even distribution shall be maintained in the event that the COSUP size is increased by decision of the General Assembly of EUCROF. Thus, the COSUP Members shall include a minimum of two (2) and maximum of three (3) representatives from each category below:

- CROs;
- Patient associations or advocates,
- Healthcare Professionals (Investigational Sites),
- Organisations producing or commercialising health products, including pharmaceutical companies, manufacturers of medical devices and biotechnology; and

- Independent experts with documented experience in one or more of the above domains[23].

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. In all cases, Members cannot also sit on any of the other decision-making bodies of EUCROF: the Executive Board, the Full Members Board, or the General Assembly.

5.2.2 Chairman and Vice-Chairman

The Chairman and Vice-Chairman of the COSUP shall be elected by and from among the Members of the COSUP. During a mandate, only one of these two functions can be occupied by a member also having an active position in a CRO. 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.

5.2.3 Membership terms

The term of office for Members of the COSUP is 3 years. A regular Member can have their term of office extended for 3 successive terms of 3 years.

The term of office of the Chairman and Vice-Chairman is also 3 years and can be extended only one time after re-election, meaning that the maximum duration a Member can fulfil the role of Chairman or Vice-Chairman of the COSUP is 6 years. The Chairman or Vice-Chairman of the COSUP, having exhausted their 6 years' term can, however, continue as a regular Member in accordance with the rules for regular Members or apply to take the role they did not previously hold.

5.2.4 Powers

The COSUP performs the following functions:

a) Reviews and assesses the applications and submitted compliance files of CROs willing to adhere to the Code and decides on the appropriate Compliance Mark for successful applicants.

b) Delivers appropriate instructions for the update of the online Public Register of adhering CROs.

c) Makes decisions regarding the selection of Auditors and registers approved Auditors in the Auditors Panel.

d) Organises and approves the allocation of Auditors to assess CROs who have applied for adherence to the Code under the audit scheme as per section 5.5.6.

e) Makes decisions regarding the selection of the Risk and Compliance Officer whose role is specified in section 5.4 hereinafter.

f) Elaborates and submits to the vote of the EUCROF General Assembly, the Compliance Marks that may be used by adherent CROs.

g) Organises and monitors the maintenance of compliance by adherent CROs at regular intervals as defined in the Code's procedures regarding the process of controlling and maintaining compliance with the Code.

[23] An example of the composition reflecting a balanced representation of Members could be: 12 members of the COSUP including:

- 1 data protection officer from a CRO, 1 compliance officer and 1 information security office from a CRO, together making 3 representatives of CROs.
- 1 chief operating officer from a patient association, 1 legal counsel who advocates for patient rights, together making 2 representatives of patient associations or advocates.
- 1 member of a national Central Ethics Committee, 1 lead researcher from a University Hospital that acts as an Investigational Site, together making 2 representatives of Healthcare Professionals (Investigational Sites).
- 1 head of privacy from a pharmaceutical company, 1 chief information security officer from a medtech company, together making 2 representatives of organisations producing or commercialising health products, including pharmaceutical companies, manufacturers of medical devices and biotechnology.
- 1 independent consultant security auditor, 1 independent consultant who is expert in de-centralised trials, and 1 director of a biobanking organisation, together making 3 representatives who are independent experts with documented experience in one or more of the above domains.

h) Establishes procedures and structures to deal with complaints about infringements of the Code or the manner in which the Code has been, or is being, implemented by CROs. In conformance with section 74 of EDPB *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*, these procedures will be publicly available on EUCROF website.

i) Investigates and adjudicates complaints about infringements of the Code by adherent CROs.

j) Takes appropriate action against a CRO in the case of an infringement of the Code or in the event that a CRO is not providing the information necessary to investigate a possible infringement of the Code to the COSUP.

k) In conformance with Article 41(4) of the GDPR, informs the competent supervisory authority of final actions taken against CROs and the reasons for taking them. In case the CRO is suspended or excluded, information of competent supervisory authority shall be performed without delay.

l) Implements procedures and structures that prevent conflicts of interests.

m) Communicates with the wider public as required to ensure appropriate transparency. For this purpose, the COSUP has the capacity to deliver appropriate instructions for the update of the EUCROF website and the corresponding EUCROF bodies shall implement such instructions with reasonable diligence.

n) Performs appropriate financial management and provides informational reporting to the General Assembly of EUCROF[24];

o) Develops and implements all relevant procedures to ensure that COSUP's operations comply with ISO Standards 17065 and 17024 and are properly documented, organises internal audits as necessary and to this end, coordinates as appropriate with the Risk and Compliance Officer, in order to achieve and maintain its accreditation by the competent authority.

p) Monitors changes in European Union data protection laws and other relevant laws and proposes relevant changes to the Code within three months of material changes in such data protection laws. For this purpose, the COSUP has the capacity to activate relevant EUCROF working groups or set-up *ad hoc* working groups as necessary.

q) Contributes to the continuous improvement of the Code by analysing records of daily practice (audit reports, complaints' handling etc...) and elaborating recommendations for improvements at the intention of the Code owner (EUCROF).

r) Reviews updates to the Code, before their submission to the competent supervisory authority by the Code owner (EUCROF).

It has to be noted that the introduction of changes to the Code is the responsibility of the Code Owner (EUCROF). The Code Owner shall inform the competent supervisory authority of the envisaged changes prior to their entry into force and as deemed necessary by the competent supervisory authority, a new approval of the Code may be necessary before entry into force of such changes.

5.2.5 Conflicts of Interest, Impartiality, and Independence

At the time of their nomination, Members of the COSUP shall complete a declaration of direct or indirect interests with organisations that have adhered or may adhere to the Code, as well as the clients of such organisations.

In addition, a procedure to declare potential conflicts of interests will be implemented before each meeting of the COSUP as a standing item on the meeting agenda. This procedure excludes the Members having a potential conflict of interest (e.g., with a CRO applying to adhere to the Code) from voting on those matters.

If the Chairman is conflicted, then the Vice-Chairman shall chair the affected part of the meeting agenda and the associated vote. If the Vice-Chairman is also conflicted, then the affected part of the meeting agenda and the associated vote shall be chaired by any other Member who does not have a conflict of interest.

The model of declaration of direct or indirect interest is annexed to the present Code in Appendix 4.

[24] The General Assembly does not exercise any control on COSUP financial management, so this reporting is only to provide information.

In conformance with section 68 of EDPB *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679,* the COSUP:

- Must remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from any person, organisation, or association.
- The COSUP shall have its own staff which are chosen by them or some other body independent of the Code Owner and the COSUP staff shall be subject to the exclusive direction of the COSUP only.
- The COSUP shall be protected from any sort of sanctions or interference (whether direct or indirect) by the code owner, other relevant bodies, or members of the code as a consequence of the fulfilment of its tasks.

The Members of the COSUP are required to sign an engagement of independence and confidentiality. The model of engagement of independence and confidentiality is annexed to this present Code in Appendix 5 and is an integral part of the Code.

Impartiality and the absence of conflicts of interests in the Members of the COSUP is managed in compliance with the requirements of ISO 17065.

5.2.6 Installation of the COSUP

Recruitment of candidates for membership to the COSUP shall be performed by an *ad hoc* working group formed by the General Assembly of EUCROF.

The creation of this *ad hoc* working group and its operations follows the standard rules applicable to all EUCROF working groups:

- Upon approval of the Full Member Board or the General Assembly of EUCROF, the Executive Board of EUCROF shall put out a call for volunteers to all its members.
- Volunteers will not get any financial compensation for their time dedicated to their participation in the activities of the *ad hoc* working group.
- Receipted travel and accommodation expenses shall be covered by the budget of EUCROF in accordance with EUCROF Financial Policy and management.
- The chairman of the *ad hoc* working group shall be elected by the participants at its first meeting.
- Given the task assigned to this working group, once initially established, this working group has full capacity to invite representatives of all stakeholders interested in the Code to participate in its activities.

The task assigned to this working group shall be the following:

- Identify and contact potential candidates;
- Document the eligibility of the candidates;
- Ensure that the resulting composition of the proposed COSUP complies with the requirements of section 5.2.1 above;
- Present the selected candidates to the General Assembly of EUCROF who will formally approve each of the candidates through a vote; and
- Once the membership is approved, ask for candidates for the Chairman and Vice-Chairman positions to present themselves from amongst the Members, and set a date for the first meeting of the COSUP and circulate the agenda which shall be for the vote on the Chairman and Vice-Chairman positions.

The candidate Chairman and Vice-Chairman shall be prepared to present their candidacy and plans to the COSUP at the first meeting of the newly installed COSUP. The COSUP shall vote on the Chairman and Vice-Chairman position at the first meeting of the COSUP, whereupon the successful candidates will be immediately installed and thereafter the working group shall be disbanded so that the COSUP can perform its tasks and exercise its powers independently.

5.2.7 Decision making

Each Member of the COSUP has one vote. Votes can be cast in writing provided they are expressed before the deadline specified each time. When voting is called to take place in a meeting of the COSUP, votes in writing can be cast up to the start time of the meeting.

Decisions of the COSUP are taken by simple majority vote of its Members, provided that the quorum is achieved.

The opinion of the Chairman on the content of a resolution is not decisive. Members can submit amendments to a resolution at the time of voting on that resolution.

If the quorum is not available, the attending representatives will decide, by simple majority of the attending representatives, either to postpone the vote to the next meeting or to issue a call for written votes to occur within 15 calendar days.

All resolutions approved by the COSUP shall be listed in a dedicated registry.

5.2.8 Meetings, quorum, and working practices

The COSUP shall meet on a regular and scheduled basis at least once every other month either in person or electronically, for example, by teleconference. The Chairman can also, at their own initiative or upon request of a Member or the Risk and Compliance Officer, call for a meeting of the COSUP at any time, as required to perform their activities.

The COSUP shall not be quorate unless the meeting is attended by at least one of the Chairman or Vice-Chairman and half of the remaining Members. If the meeting is not quorate then the meeting shall be adjourned and rescheduled until such time that a quorum can be achieved.

Meetings of the COSUP are not public but the COSUP may request external experts to provide information on relevant topics or to attend as non-voting guests to the meeting.

The agenda shall be e-mailed by the Chairman or the Vice-Chairman to all invitees, at least one calendar week before the meeting, specifying the particular items requiring a vote of the COSUP Members.

The matters discussed in each COSUP meeting shall be included in the minutes drawn up by one of the Members designated by the Chairman at the beginning of the meeting. These minutes shall be distributed to all COSUP Members, and where needed, be revised. These minutes shall be voted for approval at the latest during the following COSUP meeting.

The COSUP can determine further regulations or terms of reference in which it further lays down its working practices.

5.3 The Risk and Compliance Officer

The COSUP shall arrange the recruitment of the Risk and Compliance Officer in accordance with the Human Resources procedures of the COSUP. In particular, the COSUP shall ensure that the Risk and Compliance Officer displays the requisite experience, qualifications, professional integrity, independence, and impartiality (in particular ensuring there is an absence of conflict of interests) in order to fulfil the role.

The Risk and Compliance Officer is responsible for:

- the development and implementation of the processes, procedures, records, and templates needed for the accreditation of COSUP as a monitoring body for the Code, against ISO 17065 and ISO 17024 requirements, in the scheme of the Code requirements;
- the development of the processes, procedures, and support documentation to assess CROs' adherence with the requirements of the Code;
- the development of the education and training material for Auditor training, to evaluate their fulfilment of the requirements of the Code, the training and qualification of Auditors and their periodic performance monitoring during the periods of adherence to ensure continued compliance with the Code;

- the writing of the anti-bribery declaration that shall be signed by the Members of COSUP, the Auditors and the Risk and Compliance Officer and every other person working on the behalf of the Monitoring Body;
- the review of audit reports and, eventually, their improvement;
- the communication to COSUP of the recommendations of the Auditors as regards the assessment of a CRO following the audit scheme in the Level 2 EUCROF Code Compliance Mark process; and
- the provision of advice to COSUP, whenever it is requested.

All the audit reports shall be written in English, to make possible the review of the report by the Risk and Compliance Officer using the COSUP template in order to have uniform reporting, regardless of the country of auditee. The reports may also be translated into the national or regional (in the case of Belgium, Switzerland, Spain) languages in use.

The Risk and Compliance Officer will develop the training programme for Auditors in collaboration with the COSUP. The COSUP shall approve the training programme before its first implementation. The training programme is subject to amendments taking consideration of observable deficiencies in the implementation of the auditing process or in the audit reports.

Unexpected supervision of the Auditors may take place during their auditing to assess the way the Auditors perform their audits, to ensure their continual improvement and effectiveness.

The Risk and Compliance Officer shall have considerable experience in auditing, with more than 40 completed audits performed using a recognised ISO standard, as well as sound experience with compliance and risk, assessing audit reports, and in the qualification and training of other auditors.

5.4 The Auditors

Under certain circumstances detailed in section 5.5 of this Code, assessment of an eligible CRO’s adherence to the Code requirements may be performed by means of on-site audits (at the premises of the CRO).

To this end, the COSUP will establish a team of “Auditors” (herein also referred to as "Auditors Panel") to perform audits of applicant CROs in the manner defined by the COSUP and the Risk and Compliance Officer.

The decision to list an Auditor in the Auditors Panel is the exclusive responsibility of the COSUP and shall be documented and subject to a formal vote of the same COSUP.

5.4.1 Qualification of Auditors

The Auditors shall have documented experience in auditing ISO 9001 or ISO 27001, good knowledge of other applicable internationally recognisable standards such as ISO 27701 or NIST SP 800-53, an in depth understanding of data protection issues, an excellent knowledge of this Code’s requirements, and sufficient knowledge of the activities of CROs.

They shall be already accredited as auditors with a documented experience of more than 15 audits in the same or related fields, including audits or related working experience in organisations with activities similar to those of the CROs.

Before being assigned to their first audit mission as per section 5.4.2, the Auditors will complete three days of training with a curriculum that covers ISO 9001, ISO 27001, ISO 17024, ISO 17021-1, GDPR and this Code by the Risk and Compliance Officer and one or more Members of the COSUP, in accordance with COSUP’s Human Resources procedure.

5.4.2 Assigning an Auditor to an audit mission

When a CRO needs to be audited for compliance with the Code under section 5.5, it is the exclusive responsibility and decision of the COSUP to assign an Auditor to this audit mission.

Following its approved operating procedures, the COSUP shall identify an Auditor from the Auditors Panel subject to the requirement that this Auditor has no conflict of interest in relation with the assigned audit mission. The Auditor will then be requested to sign a "Declaration of absence of Conflict of Interest" as instructed by the COSUP.

Upon reception of this declaration, the COSUP will be entitled to formally instruct the Auditor to perform, on their behalf, the audit mission. Such instruction shall take a written form and be based on a formal resolution (through a vote) of the COSUP.

5.4.3 General conditions of audits

An Auditor assigned to an audit mission shall be given access to the preparatory documentation package collected from the concerned CRO to establish its audit plan.

The preparatory documentation package contains (a) the statement of applicability of the candidate CRO, and (b) for each of the applicable requirement, the response of the CRO on how it complies with that requirement. When appropriate, this response may require the attachment of additional documentation such as standard operating procedures (SOPs), policies or specific records.

The Auditor shall liaise with the concerned CRO within 2 weeks after the date of assignment and has a maximum of 5 weeks to agree a date of audit.

The Auditor shall send their proposed audit plan to the responsible person of the CRO at least 3 weeks before the date of audit and the CRO shall have the opportunity to ask any questions and provide suggestions for amendment of the audit plan.

The number of auditors and the duration of an audit depends on the size, the activities, and the complexity of the CRO to be audited, and it may, usually, last from one to three days.

The audit shall start by an opening meeting where the Auditors shall introduce themselves, as well as the objectives and the modalities of the audit and shall remind the audited CRO how to submit appeals or complaints as per section 5.7.1 of the Code. The responsible person of the CRO shall then introduce the involved people from the CRO and give general housekeeping information to the Auditors e.g., fire regulations and health and safety rules of the premises.

An audit should not concern individual medical records with identifiable Personal Data, but in all cases, auditors are subject to professional secrecy and shall not be authorised to remove health data from its storage location to include in audit reports.

At the end of the audit, the Auditors shall have enough time (as agreed in the audit schedule) alone to prepare a draft report with the list of identified non-conformities, areas for improvement and strengths.

Then the Auditor shall invite the CRO representatives to attend a closing meeting at the end of the audit where the Auditor shall present the key conclusions of the audit, including the listed non-conformities, areas for improvements and strengths of the CRO, together with the appropriate explanation and/or evidence for their remarks.

The auditor must communicate the audit findings in writing to the CRO. Depending on the results of the audit, the CRO shall send within five working days a Corrective Action Plan for acceptance by the Auditor.

5.4.4 Submission of the audit reports

After receiving and accepting the CRO's Corrective Action Plan, the Auditor has 5 working days to finalise the audit report including his recommendation for approval of adherence, conditional approval where there are cases of minor non-conformities that will be remedied by the CRO implementing the Corrective Action Plan, or rejection in the case of major non-conformities incapable of remedy in the Corrective Action Plan. In the case of non-conformities, the Auditor shall also attach to its report the Corrective Action Plan agreed with the CRO.

The audit report shall be signed by the Auditor and transmitted (a) to the Candidate CRO, and (b) to the Risk and Compliance Officer for their review. Appropriate electronic means shall be used for such transmission and shall include appropriate timestamping and audit trail.

The Candidate CRO and the Risk and Compliance Officer have 1 week from receipt of the audit report to provide their respective remarks, after which the Auditor shall finalise the audit report.

The final whole report package is then submitted by the Risk and Compliance Officer to the COSUP for decision.

5.4.5 Audit expenses

Auditors are paid by the COSUP, on the basis of the approved quotation and corresponding invoices provided by the Auditor. Payments are performed following the conditions defined in the Financial Policy of the COSUP.

Eligible expenses include the daily fees agreed in the quotation and travel and accommodation expenses on the basis of receipts. This total amount, including management fees charged by COSUP, shall then be charged to the audited CRO by COSUP.

5.5 Conditions of adherence

5.5.1 Eligibility

Any CRO organisation as defined in section 1.2 whose activities are listed in Appendix 1 of the present Code (section 1.7) is eligible and can adhere to the Code. This applies equally to EUCROF members and to non-members.

A CRO engaging the adherence procedure is hereinafter referred to as a "Candidate CRO".

5.5.2 Approval of adherence

The decision to approve a Candidate CRO as adhering to the Code is the exclusive responsibility of the Monitoring Body (COSUP) and shall be subject to a formal decision through a vote of the Members of the COSUP subject to section 5.2.7 of this Code.

Such decision shall only be made after review of a documentation package submitted by the CRO and payment of an application fee. This documentation package shall first be reviewed by the Risk and Compliance Officer for (a) eligibility and (b) completeness. The Risk and Compliance Officer shall add his review report to the adherence documentation package before submission to the COSUP. Where the CRO has elected to apply for a Level 2 EUCROF Code Compliance Mark, the COSUP will also be sent the final audit report by the Risk and Compliance Officer.

The decision of the COSUP shall be timestamped and documented, justification arguments explained in a written report signed by the Chairman of the COSUP and addressed to the Candidate CRO.

For Candidate CROs whose adherence has been approved but who are not members of EUCROF, they shall be required to pay the annual fee published on the EUCROF website before their adherence will be confirmed on the Public Register and such CRO shall not be entitled to their EUCROF Code Compliance Mark before the fee is paid.

5.5.3 Public Register

A register of adherent CROs shall be available for on-line consultation by the public in EUCROF website. This registry is herein referred to as the “Public Register" and it is the only official listing of adherent CROs.

It is the exclusive responsibility of the COSUP to maintain and update this Public Register appropriately. Changes in the adherence status of a given CRO shall be reflected in the Public Register without undue delay and no later than five (5) working days after the change occurred. This time period shall be published on EUCROF website and the Public Register.

Every record of the Public Register shall be timestamped and contain all essential information regarding the adherence of every listed CRO. Examples of essential information are; EUCROF Code Compliance Mark (declarative or audit based), date of approval and reference to the corresponding COSUP decision, next renewal date etc...

5.5.4 Different levels of adherence

The Code provides for different levels of adherence recognition for adherent CROs. The different levels of adherence recognition reflect only the levels and method of evidence that are submitted to the COSUP. Adherent CROs must comply with all provisions of the Code regardless of the level of adherence recognition for which the Candidate CRO is applying.

The level is the exclusive choice of the Candidate CRO and this choice shall be made before the adherence procedure is engaged as it will determine the application procedure. The COSUP will in both cases have the ultimate responsibility for deciding whether or not to grant adherence to the CRO.

5.5.5 Level 1: a declarative adherence procedure

In the declarative adherence procedure (or "Level 1 Procedure"), the Candidate CRO completes and generates the adherence file alone and the COSUP only intervenes after the CRO has submitted its file.

Under this Level 1 Procedure, the Candidate CRO shall complete an "organisation profile" and shall provide detailed documentation proving their compliance with all applicable measures in accordance with their Statement of Applicability. The documentation is accompanied by an inventory of the submitted evidence in a format referred to as the “compliance questionnaire”.

The models of "organisation profile" and "compliance questionnaire" are documents validated by the COSUP and shall be accessible through the website of EUCROF. The “compliance questionnaire” includes the applicable requirements of the Code.

In addition to the above, the applicant CRO must sign a “Declaration of Accuracy and Completeness” of the information contained in its adherence file. The CRO is then authorized and must send its adherence file via the EUCROF website.

The adherence file is reviewed by the Risk and Compliance Officer for (a) its eligibility and (b) its completeness and transmitted to the COSUP with its review report.

The COSUP analyses the eligibility of the Candidate CRO on the basis of the adherence file and the report of the Risk and Compliance Officer. The COSUP determines whether each applicable Code requirement according to the CRO's Applicability Statement has been sufficiently addressed and whether the documentation provided allows the COSUP to monitor the CRO's compliance. The COSUP has the power to require the applicant CRO to provide additional evidence of compliance, e.g., more documentation. The adherence file will be processed by the COSUP within the maximum deadline published on the EUCROF website, and a decision will be communicated to the candidate CRO in accordance with section 5.5.2.

The COSUP will retain responsibility for, ultimately, deciding on whether or not to grant its recognition of the Candidate CRO’s adherence.

At any point in the period of 3 years that the adherent CRO’s EUCROF Code Compliance Mark is extant or in case of complaint against the CRO, the COSUP has the right to appoint an Auditor, as per section 5.6.2 to verify on-site the enforcement of the "Declaration of accuracy and completeness" and the effectiveness of the adherence procedure and that the needed documentation is properly maintained or retained.

At any time during the three-year period that the EUCROF Code Compliance Mark is valid, or in the event of a complaint against the CRO, the COSUP has the right to mandate an Auditor, in accordance with section 5.6.2, to verify on site the implementation of the “declaration of accuracy and completeness” and the effectiveness of maintaining the conditions of adherence.

5.5.6 Level 2: third party assessment

This procedure requires an on-site audit of the Candidate CRO (“Level 2 Procedure”). This on-site assessment shall only be performed by a one or more Auditors (their number depending on the size of the Candidate CRO) selected and mandated by the COSUP from the Auditors Panel.

The main steps of the Level 2 Procedure shall be the following:

1 The Candidate CRO shall register his application through the EUCROF website and complete the adherence documentation package that consists of (a) the "organisation profile" and (b) the "compliance questionnaire" also used for "Level 1 Procedure".

2 This preliminary documentation package shall be reviewed by the Risk and Compliance Officer for (a) eligibility and (b) completeness and transmitted to the COSUP together with its review report.

3 The COSUP will then allocate one or more Auditor(s) from the Auditors Panel as per the applicable operating procedures.

4 Once confirmed, the Auditor will release a quotation based on the transmitted documentation. This quotation shall be approved by the Candidate CRO in writing. Upon approval, the name and CV of the Auditor will be transmitted to the Candidate CRO. The Auditor shall receive from the COSUP a written instruction to perform the corresponding audit.

5 The Auditor shall then organise and perform its audit pursuant to the conditions defined in section 5.4.3 of this Code and release the corresponding report with their recommendation to the Risk and Compliance Officer and the COSUP on the approval, or conditional approval, or rejection.

6 The Risk and Compliance Officer can then request clarifications from the Auditor. Once all eventual clarifications obtained, the Risk and Compliance Officer prepares its Review Report and forwards to the COSUP the final whole audit documentation for insertion in the agenda of a next meeting of the COSUP which will make the final decision about whether or not to grant its recognition of the Candidate CRO's adherence.

7 The decision will be provided to the Candidate CRO in accordance with section 5.5.2.

5.5.7 Conditions to use Compliance Marks

EUCROF will develop official EUCROF Code Compliance Marks for each level. Such Compliance Marks shall only be used by the CROs listed in the Public Register.

Detailed rules of using such Compliance Marks will be developed in a guidance document validated by the COSUP and EUCROF.

Misuse, as well as breach of the aforementioned conditions will constitute an infringement of the Code and may result, at the discretion of the COSUP, in fines or penalties.

If, after previously being verified compliant by the COSUP, a dispute concerning non-compliance of an adherent CRO arises, the use of the Compliance Mark by the CRO should be suspended until the complaints procedures pursuant to section 5.7 comes to a resolution. After receiving a final outcome of non-compliance with the Code, the CRO must immediately cease to use the Compliance Mark.

5.6 Monitoring and enforcement

5.6.1 Validity of adherence

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. Before the end of each 3-year period the adherent CRO shall apply for renewal of its adherence to the Code through the same procedures described in section 5.5. In the case that a CRO decides not to continue its adherence, it shall formally notify the COSUP of its intention to withdraw from adherence using the revocation mechanism published by the COSUP. If no notification of intent to withdraw or renewal has been received, the COSUP shall remove the CRO from the Public Register in accordance with the guidance document as per section 5.5.7.

5.6.2 Monitoring

During an approved 3 years period, the compliance of any CRO that has been declared as adhering to the Code shall be monitored by the COSUP once every twelve months and at any time in the event of:

a) Reported major non-conformities, or repeated minor non-conformities;

b) A complaint by a data subject or any other interested stakeholder;

c) Significant changes occurring to the adherent CRO; or

d) In reaction to an adverse media report or anonymous feedback about a CRO listed as adhering to the Code in the Public Register.

Such monitoring shall be performed by an Auditor according to the Compliance Control Procedure approved by the COSUP. This Compliance Control Procedure and its eventual amendments shall be publicly available on the EUCROF website. The final decision with regard to the monitoring activities to determine compliance or non-compliance of an adherent CRO and the related responsibility for enforcement are taken by the COSUP on the basis of the audit report.

Interim annual monitoring focuses on the improvement points listed from previous audits or non-conformities identified through the internal audits carried by the adherent company itself in the frame of its ISMS. In addition, the auditor performs additional auditing on the basis of his knowledge of the company and on a sampling approach. Notwithstanding the aforementioned, the adherent CRO must comply with all requirements of the Code at all times and the COSUP may at any time perform a full assessment.

5.6.3 Enforcement

If the COSUP becomes aware of any non-compliance of an adherent CRO, the COSUP can require the CRO to take specific measures ceasing any further infringement and adopting remediation measures within a time period that the COSUP shall define. If those measures are not adopted within this defined period of time, the Compliance Mark of the adherent CRO shall be suspended. The COSUP shall take the appropriate action with regards to the sanctions and remedies pursuant to section 5.8.

In the event that the decision of compliance of a CRO is revoked, the COSUP shall (a) inform the competent supervisory authority without delay and (b) immediately remove that particular CRO from the Public Register. The CRO shall immediately cease to make reference to the Code or the Compliance Mark in any of its documentation or publications, including its website.

5.7 Complaints Handling and Procedures

5.7.1 Complaints of CROs against decisions of the COSUP

CROs may file a complaint against any decision taken by the COSUP.

Complaints in relation to or appeals against any rejection of a Candidate CRO's application under the Level 1 Procedure or Level 2 Procedure shall be addressed to the Risk and Compliance Officer using the EUCROF website. The COSUP shall be informed of the receipt of such complaint within 2 working days.

The Risk and Compliance Officer reviews the complaint or appeal and shall produce a review report within 2 weeks of receipt of the complaint or appeal. During this phase, the Risk and Compliance Officer may ask any additional clarification from the concerned CRO, and Auditor if the Level 2 Procedure was followed. The review report together with the initial complaint or appeal and any eventual additional information provided by the CRO at the request of the Risk and Compliance Officer shall then be transmitted to the COSUP and the issue incorporated in the agenda of the next meeting of the COSUP.

The COSUP can then take any decision it judges the most appropriate; including agreeing with the appeal of the concerned CRO, asking for further evidence of compliance, launching a new compliance verification process or confirmation of the prior rejection.

5.7.2 Complaints against any adherent CRO

If an interested stakeholder has reservations regarding a CRO's compliance, that person is encouraged to contact the CRO first in order to obtain a mutually satisfactory solution. However, the interested stakeholder can directly submit a complaint to the COSUP, without contacting the concerned CRO.

Such a complaint may be filed by any party, regardless of whether or not such party is a customer of the respective CRO, in their own name or anonymously through the EUCROF website.

The COSUP shall review the complaint, require the CRO to provide any relevant information for the purposes of fact finding, apply the Compliance Control Procedure as described in section 5.6.2, and initiate a complaint handling process to determine whether the complaint was justified. In case the COSUP concludes that the complaint was justified, the COSUP will take appropriate actions to stop any further non-compliance of the adherent CRO.

Complaints shall be investigated and resolved by the COSUP promptly and within one month, extendable by two further months taking into consideration the complexity of the complaint, the seriousness of the complaint, and the risk-level of the complaint (in particular the impact to the data subject(s)) as specified in the Compliance Control Procedure or any other appropriate documentation.

The COSUP will decide on possible sanctions and remedies in accordance with the sanctions and remedies provided under this Code.

5.7.3 Costs and Fees related to Complaints

5.7.3.1 Costs for Complainants

As a rule, complaints can be submitted free of costs for the complainant. However, the COSUP may define costs for complainants, where appropriate, to prevent potential abuse due to manifestly unfounded or excessive complaints, in particular if they are recurring.

5.7.3.2 Costs for CROs

Additional costs related to any upheld complaints related to an adherent CRO shall be borne by the concerned CRO; such additional costs may include expenses of additional on-site audits or external expert review of the complaint file to substantiate the complaint.

If considered as justified to maintain sustainable financial operations, the COSUP has full capacity to propose the inclusion in its annual budget, of additional complaint handling fees. In this case, when the annual budget is approved by the EUCROF General Assembly, such additional fees shall be made public and known to all adherent CROs.

5.8 Sanctions, remedies and notification of the supervisory authority

Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII of the GDPR, the COSUP takes appropriate actions with regards to sanctions and remedies against any adherent CRO who is found to be non-compliant with the requirements of this Code or rejects cooperation with the COSUP in performing their tasks under this Code and GDPR appropriately.

5.8.1 Sanctions and Remedies

An adherent CRO that after investigation in accordance with the procedures in section 5.6.2 and section 5.7.2 is found to be non-compliant with any requirement of the Code, shall be subject to appropriate sanctions and remedies. The COSUP shall consider the following aspects when assessing the appropriateness of each action:

- Severity of non-compliance with regards to the potential impact on level of data protection related to the Personal Data processed, including the potential impact on the freedoms and rights of data subjects.
- Liability of the CRO with regards to whether the CRO intentionally disrespected the requirements of the Code or negligently misinterpreted them.
- Frequency of non-compliance; has it been the first breach or have there been similar incidents before.

Based on the aforementioned criteria the COSUP shall impose sanctions and remedies that can be one or any combination of the following:

- Non-public but formal reprimand.
- Public announcement of the non-compliance and subsequent formal reprimand, including facts and reasoning.
- Temporary or permanent revocation of CRO from the Public Register and the related revocation of its entitlement to use the Compliance Mark.

5.8.2 Guidelines for Sanctions and Remedies

To safeguard comparability and coherency of sanctions and remedies imposed to CROs, the COSUP will develop and implement guidelines governing sanctions and remedies or ranges thereof to be imposed on CROs.

Those guidelines shall be drafted, approved and frequently reviewed by the COSUP taking into account the practical experiences of the COSUP with regards to cases of non-compliance by adherent CROs.

The guidelines shall list and document, with examples, all envisaged types of non-compliances as well as the corresponding sanctions and / or remedies to be expected. The determination of sanctions and remedies shall

consider any useful aspect in order to assess the appropriateness of any sanction and remedy, as defined in section 5.8.1.

The COSUP may at any time deviate from the available guidelines, provided that the COSUP explicitly refers to its deviation in its decision together with appropriate reasoning why such deviation was deemed a necessity. Such a decision shall result in a review of the guidelines.

5.8.3 Notification of and cooperation with the supervisory authorities by the COSUP

Without prejudice to Article 41(4) of the GDPR, the COSUP shall proactively and in due time notify the competent supervisory authority of sanctions and remedies imposed on CROs and the reasons for taking them, including non-public but formal reprimands.

If any supervisory authority indicates to the COSUP that they are concerned that actions taken by the COSUP fall short of what supervisory authorities expect as appropriate action, the COSUP will take this feedback into account for any future decision to be taken.

In all instances, the COSUP shall cooperate with the supervisory authorities by providing full information related to the circumstances from which the sanction arose and the rationale for decisions taken by the COSUP. The COSUP shall respond promptly to any requests for further information and shall implement the recommendations or requirements and additional actions that the supervisory authorities deem necessary.

5.9 Finances

5.9.1 Financial Management

The COSUP is responsible for managing its annual budgets in the most appropriate way. It is a task of the Chairman to organise financial management in the most efficient way. This task includes:

- Drafting a provisional annual budget of the COSUP for the forthcoming year and submitting it for approval by the COSUP.
- Reporting on the execution of the annual budget of the past year and have the annual statement approved by the COSUP.
- Providing financial information to the General Assembly of EUCROF in order to allow EUCROF to fulfil its own financial reporting in regard to the subsidies provided to COSUP.
- Ordering all required payments in relation with the execution of the budget of the running year and in the frame of the approved budget.

Upon proposition of the Chairman, the COSUP may nominate one of its Members to carry out the above tasks on behalf and under the responsibility of the Chairman. Such nomination shall be subject to a vote of the COSUP.

The annual COSUP budget shall cover the costs for secretarial support, Risk and Compliance Officer, the Auditors Panel, IT Platform and the COSUP's activities.

5.9.2 Eligible expenses of the COSUP

Expenses of the COSUP that are eligible are the following:

a. A compensation fee will be allocated to the Members for their participation to the activities of the COSUP. The amount of the compensation fee depends on (a) the role of the Member – Chairman, Vice-Chairman, regular Member and (b) the type of meeting (physical meeting or teleconference call).

b. Travel and accommodation expenses engaged in the execution of their role are reimbursed to the Members on the basis of receipts and in accordance with the conditions defined in the Financial Policy of EUCROF.

c. Any other expenses required for efficient operation of COSUP such as rental of meeting rooms, technical means (teleconference call means ...), purchase of reports on subject-matters of interest etc...

5.9.3 Annual fees

The operating costs of the COSUP are covered by the annual fees paid by adhering CROs, whether they are affiliated to EUCROF or not and, if necessary, by the annual subsidy from EUCROF.

The amount of the annual fees paid by the CROs not affiliated with EUCROF may be different from the amount paid by affiliated CROs. The amount of annual contributions was set by the EUCROF General Assembly and may be revised each year by the same. The amount of contributions is published on the EUCROF website.

In accordance with point 5.4.5 and point 5.7.3.2 of this Code, costs related to audits and/or handling complaints will be directly charged to the CRO concerned, in addition to the regular annual fee.

5.9.4 Control and publication

The accounts of the COSUP will be incorporated in the annual statement of accounts of EUCROF under separate analytical lines and will be publicly available.

The Chairman of the COSUP shall liaise as necessary with the Treasurer of EUCROF to publish timely reports on the annual budget of the elapsed year.

The accounts of the COSUP will be subject to same control and approval rules as the general EUCROF budget.

5.10 Code Review and Update

The Code Owner shall undertake, every two (2) years, a periodic review of the content of the Code of Conduct, so that it can be amended and incorporate the modifications needed to facilitate compliance with data protection rules in Clinical Research in a constantly changing environment. Those periodic reviews are without prejudice to the possible review of the Code whenever required by new legislative or case-law developments or technological developments.

The Code Owner shall determine if a review is required outside of the regular review cycle, and at its discretion can seek consultation with COSUP and the competent supervisory authority in deciding whether a review is required.

In all cases, the Code Owner shall be responsible for making the changes to the Code.

The modified Code shall be reviewed by the competent supervisory authority and where the changes are substantial, may need to be sent for re-approval in accordance with the Guidelines of the European Data Protection Board. Where the changes are administrative in nature e.g., to correct addresses, spelling issues or cross references, these may be published without approval from the competent supervisory authority.

The Code Owner shall publish any new approved version of the Code on the EUCROF website no less than five (5) working days after approval and shall send a notification to all Code adherents and candidates within five (5) working days of publishing the new version. The Code Owner shall provide both the new version of the Code with a summary of the last changes made and shall also provide the redline showing the changes made in order to simplify the review process for stakeholders.

All adherent CROs shall have 60 days from the effective date of the new version to implement the changes. After that 60-day transition period, the Auditor of the COSUP shall perform spot checks on adherent CROs whose EUCROF Code Compliance Mark is not due for renewal within 6 months of the effective date in order to monitor that adherent CROs have transitioned to the new version.

The next renewal audit for the adherent CRO shall be based on the version in force and it will be considered a finding if the CRO has not implemented the then current version of the Code.

Lastly, the Code is not a static instrument, but one that may undergo successive modifications to adapt it to new interpretative criteria in the decisions of supervisory authorities, the latest case-law precedents and to the needs that may be raised by the adherent entities as a consequence of technological and scientific development in the fields regulated by the Code.

Appendix 1 List of Concerned Supervisory Authorities

(1) Austria	Österreichische Datenschutzbehörde Barichgasse 40-42 1030 Wien https://www.dsb.gv.at/
(2) Belgium	Autorité de la protection des données Gegevensbeschermingsautoriteit (APD-GBA) Rue de la Presse 35 – Drukpersstraat 35 1000 Bruxelles – Brussel https://www.autoriteprotectiondonnees.be/ https://www.gegevensbeschermingsautoriteit.be/
(3) Bulgaria	Commission for Personal Data Protection 2, Prof. Tsvetan Lazarov blvd. Sofia 1592 https://www.cpdp.bg/
(4) Croatia	Croatian Personal Data Protection Agency Martićeva 14 10000 Zagreb http://www.azop.hr/
(5) Cyprus	Commissioner for Personal Data Protection 1 Iasonos Street, 1082 Nicosia P.O. Box 23378, CY-1682 Nicosia http://www.dataprotection.gov.cy/
(6) Czech Republic	Office for Personal Data Protection Pplk. Sochora 27 170 00 Prague 7 http://www.uoou.cz/
(7) Denmark	Datatilsynet Carl Jacobsens Vej 35, 2500 Valby http://www.datatilsynet.dk/
(8) Estonia	Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon) Tatari 39 10134 Tallinn http://www.aki.ee/
(9) Finland	Office of the Data Protection Ombudsman P.O. Box 800 FIN-00521 Helsinki http://www.tietosuoja.fi/en/

(10) France	Commission Nationale de l'Informatique et des Libertés – CNIL 3 Place de Fontenoy TSA 80715 – 75334 Paris, Cedex 07 http://www.cnil.fr/
(11) Germany	Federal Authority: Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Husarenstraße 30 53117 Bonn http://www.bfdi.bund.de/ State Supervisory Authorities: The full list of State Supervisory Authorities can be found here - https://www.datenschutzkonferenz-online.de/datenschutzaufsichtsbehoerden.html
(12) Greece	Hellenic Data Protection Authority Kifisias Av. 1-3, PC 11523 Ampelokipi Athens http://www.dpa.gr/
(13) Hungary	Hungarian National Authority for Data Protection and Freedom of Information Szilágyi Erzsébet fasor 22/C H-1125 Budapest http://www.naih.hu/
(14) Ireland	Data Protection Commission 21 Fitzwilliam Square Dublin 2 D02 RD28 Ireland http://www.dataprotection.ie/
(15) Italy	Garante per la protezione dei dati personali Piazza Venezia, 11 00187 Roma http://www.garanteprivacy.it/
(16) Latvia	Data State Inspectorate Blaumana str. 11/13-15 1011 Riga http://www.dvi.gov.lv/
(17) Lithuania	State Data Protection Inspectorate A. Juozapaviciaus str. 6 LT-09310 Vilnius http://www.ada.lt/
(18) Luxembourg	Commission Nationale pour la Protection des Données 1, avenue du Rock'n'Roll L-4361 Esch-sur-Alzette http://www.cnpd.lu/

(19) Malta	Office of the Information and Data Protection Commissioner Second Floor, Airways House High Street, Sliema SLM 1549 http://www.idpc.org.mt/
(20) Netherlands	Autoriteit Persoonsgegevens Bezuidenhoutseweg 30 P.O. Box 93374 2509 AJ Den Haag/The Hague https://autoriteitpersoonsgegevens.nl/nl
(21) Poland	Urząd Ochrony Danych Osobowych (Personal Data Protection Office) ul. Stawki 2 00-193 Warsaw https://uodo.gov.pl/
(22) Portugal	Comissão Nacional de Protecção de Dados – CNPD Av. D. Carlos I, 134, 1º 1200-651 Lisboa http://www.cnpd.pt/
(23) Romania	The National supervisory authority for Personal Data Processing B-dul Magheru 28-30 Sector 1, BUCUREŞTI http://www.dataprotection.ro/
(24) Slovakia	Office for Personal Data Protection of the Slovak Republic Hraničná 12 820 07 Bratislava 27 http://www.dataprotection.gov.sk/
(25) Slovenia	Information Commissioner of the Republic of Slovenia Ms Mojca Prelesnik Dunajska 22 1000 Ljubljana https://www.ip-rs.si/
(26) Spain	Agencia Española de Protección de Datos (AEPD) C/Jorge Juan, 6 28001 Madrid https://www.aepd.es/
(27) Sweden	Datainspektionen Drottninggatan 29 5th Floor Box 8114 104 20 Stockholm http://www.datainspektionen.se/

Appendix 2 Classes of services in scope of this Code

For each class of service below, there is a table that describes an overview of the subject matter, purpose, nature, duration of the processing, and the types of Personal Data. For the sake of clarity, the duration of the processing below is only indicative and specific retention period is defined by the data controller. Some Personal Data of Sponsor staff and CRO staff may always be processed by the CRO as a controller in the context of business communication for the delivery of the service however such processing remains out of the scope of this Code as stated in section 1.9.2.

Where it is not envisaged that there will be any processing of Personal Data during a particular class of service, this is indicated as not applicable (NA). This may be the case where the class of service is relevant for defining how Personal Data is to be collected and used in a different class of service, but there will not be any Personal Data processed at that stage; for example (2) ICF design & information leaflet.

The tables and their contents are intended to be general guidance and are not intended to be an exhaustive list. Individual interpretation of a CRO's particular situation is advised and where necessary, different conclusions can be accommodated within the use of this Code and shall be reflected in the Data Processing Agreement.

(1) Synopsis, protocol and CRF design

This first Study setup process relates to the design of the Study protocol (defines the purpose and means including the justification of the collection of sensitive data) and the CRF (identifies the data to be collected).

Subject matter of processing:	Development of guidelines (protocol), project plans, data collection forms including case report forms (CRF).
Purpose of the processing:	Setting up the framework of evidence for privacy by design, including integration of data minimisation, purpose limitation, and confidentiality principles.
Nature of the processing:	Processing of Personal Data of Study Subjects is not envisaged.
Types of Personal Data:	NA
Duration of the processing:	NA

(2) ICF design & information leaflet

Refers to all activities carried out to design the information and/or Informed Consent Form (ICF) for the Study Subjects according to the type of Study and the applicable regulations.

Subject matter of processing:	Development of information for Study Subjects about Study-related data processing.
Purpose of the processing:	Compliance with the right to information of Study Subjects.
Nature of the processing:	Processing of Personal Data of Study Subjects is not envisaged.
Types of Personal Data:	NA
Duration of the processing:	NA

(3) Site selection and contract

Refers to all activities related to the selection of Investigational Sites that would potentially participate in a Clinical Study, including in context of a feasibility Study, up to the signature of the contract with the Investigational Sites. The concerned service may be referred to as "site feasibility", "site identification", and "Investigator selection". CROs arranging Investigator meetings should refer to class of service (23) Arrangement of Investigator meetings.

Subject matter of processing:	Collection and analysis of Personal Data of Healthcare Professionals.

Purpose of the processing:	Selection of Healthcare Professionals qualified and capable of performing Investigator's tasks; assessment of compensation and remuneration.
Nature of the processing:	Collection/obtainment, transfer/transmission, storage, analysis, deletion/destruction.
Types of Personal Data:	Healthcare Professionals: surname, name, gender, date of birth, signature, postal address, electronic and telephone contact details, bank details; education: qualification(s); professional life (including professional background, method and type of practice, necessary elements for assessing the knowledge they have for conducting the Research); where applicable, registration number in the shared register of Healthcare Professionals; total compensation and remuneration received; participation in other Studies; training schedules, performance.
Duration of the processing:	From the bid defence meeting to completion of site initiations, site identification may continue throughout the Study.

(4) Data collection

Refers to all activities performed by the CRO related to the collection of data required for the purpose of the Clinical Research.

Subject matter of processing:	Accumulating databases of Clinical Study Data for conducting Research.
Purpose of the processing:	Enabling main purpose of Research; identification of individuals as Study Subjects.
Nature of the processing:	Collection/obtainment, transfer/transmission, storage, analysis.
Types of Personal Data:	Study Subjects: data concerning health; photographs and/or video and/or voice recordings not enabling the research subjects to be identified, e.g., masking the face, the eyes, distinctive characteristics except if such features are strictly necessary for the purpose of the clinical research , dates pertaining to the conduct of the Research, i.e., enrolment date and visit dates; ethnic origin, if scientifically justified and necessary to comply with Study objectives; genetic data strictly necessary to comply with the research objectives or purposes, not enabling the direct or indirect identification; marital status; level of education; socio-professional category; professional life, e.g., occupational exposure; affiliation to social security, (excluding registration number in the national identification directory of natural persons), supplementary insurance (mutual, private insurance); participation in other research or studies, in order to ensure compliance with the inclusion criteria; consumption of tobacco, alcohol and recreational drugs; lifestyles and behaviours, assistance (domestic help, family), physical exercise (intensity, frequency, duration), diet and eating habits, leisure pursuits; lifestyle, e.g., urban, semi-urban, traveller, sedentary; accommodation private house or block of flats, floor, lift, etc.; sex life; vital status, etc.
Duration of the processing:	Pre-screening until Study termination/withdrawal or until the Study product receives a marketing authorisation or until two years after the final publication of the Research results; or where there is no publication, until the final report of the Research has been signed.

4.1 Data collected directly from subjects/proxies

Refers to all processes where data are collected directly by the data subject himself and / or a proxy.

Examples:

- Data collected by CRO through face to face, online, phone interviews using recordings, electronic/ paper transcriptions.
- Data collected by CRO via telephone platforms: telephone questionnaires (PRO) for varied purposes including quality of life (QoL), pharmacoeconomic assessment, surveys on burden of disease, satisfaction with treatment, tolerability, screening questionnaires to detect safety concerns, evolution of symptoms, efficacy of risk mitigation strategies such as patient educational programs, pre-screening for inclusion, in a Study. Such assessments may either be performed independently from Investigators (control of influence bias thus increased data quality; no added value to have the assessment performed by an HCP) or in collaboration with Investigators, e.g., an event of interest detected through a contact will trigger an alert to Investigator or Study Subject for contacting the Investigational Site.
- Data collected by the CRO from the patients in real life conditions through ePRO, eCOA or other electronic media (EDC, smartphone, tablet) or through paper.
- Data collected in the frame of an eConsent procedure and tools.

4.2 Data collection by Healthcare Professionals through CRF (paper or electronic)

Refers to all processes where data are collected by Investigational Sites' staff (HCP) through case report forms (CRF).

4.3 Data collection from other data sources

Refers to all processes where data are collected from external sources: Electronic Health Records (EHR), nation-wide registries, local labs etc.

This type of data collection is seen particularly in the context of "real life" Studies.

(5) Monitoring

Refers to all activities performed by the CRO in the frame of monitoring of the Study. The monitoring process strives to fulfil three purposes to:

- Protect the rights and well-being of human Study Subjects,
- Conduct the Study in compliance with the protocol, GCP or other applicable standard and applicable regulatory requirements,
- Verify the accuracy and completeness of Clinical Study Data.

Subject matter of processing:	Comparing source records and completed data collection forms, ensuring proper completion and storage of ICF, safety reporting.
Purpose of the processing:	Verification of accuracy of data transfer from source records to Study data collection forms, of appropriate authorisation to processing and participation.
Nature of the processing:	Collection/obtainment, review, access, transfer/transmission, analysis, storage, deletion/destruction.
Types of Personal Data:	Study Subjects: same as for (4) Data collection.
Duration of the processing:	From first patient enrolled to CRF database lock.

Monitoring activities are usually conducted according to three different approaches as detailed below.

5.1 On-site monitoring

During on-site monitoring visits, the Study monitor is supposed to check, at least, the informed consent documentation and the patient medical file in order to assess the accuracy and completeness of reported Clinical Study Data. During those visits, the Study monitor has access to directly identifiable subjects' data. In such a way, this data processing activity requires specific attention in order to protect the Study Subject from any disclosure of their sensitive data.

5.2 Remote monitoring (also known as remote source data verification - rSDV)

Remote monitoring is evaluation carried out by monitors at a location other than the Investigational Sites with the objective to select, initiate, monitor, or close out Sites. It includes monitoring activities with focus on verifying critical data, including source data, and critical processes.

Remote monitoring intensively uses virtual environments where data/information can be collected through interview/questions and/or source documents could be uploaded by Investigational Site staff. Remote monitoring should be compliant with country-specific requirements and is subject to the permission/agreement of Investigational Sites.

The Sponsor should justify and document the justification and processes to be followed for the use of remote monitoring in general and in particular for remote source data verification. Moreover, the European and national guidance should be followed, and CROs should refer to the European Data Protection Board Guidelines and national standards published by supervisory authorities and other European guidelines, such as those published by the European Medicines Agency[25].

The Sponsor is responsible for the decision to perform remote monitoring. CRO is in the position to provide recommendations on whether the remote monitoring should be set up. As in most cases documents are leaving the Investigational Site, additional security measures must be specified and organised.

5.3 Centralised monitoring (data management)

Centralised monitoring is a data-oriented activity where data managers execute checks on data and provide indicators and deep data analysis to Study monitors. Monitors then execute monitoring (on-site and / or remote, if justified) to solve detected issues.

(6) Medical monitoring

Medical monitoring services vary according to Study design and regulatory classification. Medical monitoring is regulated for Clinical Studies.

Such services may include the following activities:

- Participation in Study steering committees and integration of expertise as appropriate;
- Development and/or review of protocol and Study documents (initial and amendments);
- Participation in Study feasibility assessment and Investigational Site selection;
- Study stakeholder training including participation in Investigators meetings with a focus on IMP and medical aspects of the protocol;
- Day to day problem-solving and medical guidance on Study related issues to the project team, e.g., specific Site questions for protocol clarification; completion of the CRF, safety-related management issues; for interventional studies, check patient eligibility per protocol and review protocol deviations.
- Close monitoring of Clinical Study database from a safety perspective.
- Provide medical input on safety data and case narratives.
- Review data listing and coding for medical sense.
- Review and comment on Clinical Study Data analysis and outcomes (SAP, CSR, publications).

Subject matter of processing:	Communication with regulatory authorities, ensuring compliance with regulatory requirements, evaluation of eligibility of Study Subjects for entering/continuing participation.
Purpose of the processing:	Demonstrating accountability for appropriate management of health-related risks, analysis of impact from the investigational product on well-being of Study Subjects.
Nature of the processing:	Collection/obtainment, transfer/transmission, analysis, storage.

[25] Recommendation paper on decentralised elements in clinical trials by EMA, Version 01, 13 December 2022

Types of Personal Data:	Study Subjects: same as for (4) Data collection.
Duration of the processing:	First patient enrolled, to clean-up of safety monitoring databases and CRF database lock/transfer of trial master file.

(7) Pharmacovigilance (PV) and safety reporting

CROs can provide a large spectrum of services contributing to the safety of medicinal products and medical devices. Services are performed either in post-marketing setting (spontaneous reporting system outside a Study and other services such as systematic literature review and signal detection) and/or in Studies or other organised data collection systems that do not qualify as Clinical Studies (solicited collection of safety information).

Typical procedures managed by PV teams in Studies include:

- guidance on Adverse Events (AEs) collected during the Study and rules for reporting by Investigational Site to PV team;
- individual case safety report management (including acknowledgment of receipt of individual AE reports, case triaging for duplicates, recording in safety database, AE report quality control and query, causality assessment and case narrative writing); and
- Submission of valid cases to competent authorities as appropriate.

These activities are highly regulated. They require the use of a safety database independent from Clinical Study database, allowing proper case management and electronic submission of valid cases to regional databases (typically, EudraVigilance in EU).

Besides individual case management and submission, Pharmacovigilance requires generation of periodic aggregate reports (DSURs, PSURs). Case processing may require direct nominative contacts with reporters (consumers and Healthcare Professionals) but submission to authorities is managed in a de-identified way.

Subject matter of processing:	Same as (6) Medical monitoring.
Purpose of the processing:	
Nature of the processing:	
Types of Personal Data:	
Duration of the processing:	

(8) Direct-to-patient (DtP) services

Supplementary patient services that will require processing of the administrative identifying data of the Study Subjects (surname, name, postal address, electronic and telephone contact details, bank details).

Examples of DtP services that can be provided by a CRO:

- Travel arrangements, including plane, train, taxi, special transport, e.g., Crohn disease patients; accommodation bookings; and related reimbursement of transport costs for the Study Subjects and/or the payment of allowances;
- Follow-up of the persons concerned as specified in the research protocol, e.g., sending a text message [SMS] to complete an online questionnaire, activating a computer account to use a linked application;
- Patient engagement into Study, e.g., a CRO employs an online platform or elsewise through which potential Study Subjects could receive reference to a closest medical site; medical site will perform final eligibility assessment and enrolment;
- Delivery of the health products, equipment, e.g., dialysis machines;
- Delivery and home collection of samples required for the Research;
- Home nursing services;

- Food catering, e.g., anorexic patients requiring a special diet;
- Companion services at patient visits to the hospital, including fast-pass in hospital queues, supplying food (special dietary restrictions, following sample withdrawal);
- Psychological support by professionals, additional explanations for a Study (organisation; use of a device);
- Patient interviewing, e.g., advocacy functions, requiring interaction with patients and families, e.g., E-products allowing direct interaction with patient via online platforms or electronic messaging systems, including electronic patient reported outcomes (ePRO); and
- Telephone platforms allowing direct interaction with patient; telephone questionnaires for varied purposes, including PROs, quality of life (QoL) questionnaires, pharmacoeconomic assessment, etc.

Subject matter of processing:	Communication for the delivery of the service.
Purpose of the processing:	Providing support to Study Subjects that is related to the administrative activities that are needed or complementary to the Research and are beyond the essential Research purpose.
Nature of the processing:	Collection/obtainment, transfer/transmission, storage, de-identification (pseudonymisation, anonymisation, aggregation, masking, removal of data elements), deletion/destruction.
Types of Personal Data:	Depends on type of service, and will imply combination of minimal health data, e.g., disease name, general information on the individuals' specific health condition; with identifying data of Study Subjects, e.g., surname, name, postal address, e-mail address, bank details; transportation services, location, reimbursement costs, etc.
Duration of the processing:	Study Subject's data received to end of service delivery with consequent deletion of identifying data; duration of retention of aggregate data for financial accountability shall be defined by the applicable national laws.

(9) Data management

Refers to the following activities:

- Development of a Data Management Plan (DMP) before data management activities start to describe the processes used to manage the data throughout the conduct of the Study.
- Process for the development of data collection systems for paper based, electronic and hybrid systems; this covers Electronic Data Capture (EDC) software management from configuration, maintenance and change control during production phase.
- Quality control of the database for paper documents (including defining sample, data and variables to be checked and acceptable threshold as well as actions to be taken according to results).
- Ongoing data cleaning process during the Study from the first data captured to the final database locked. This will be done by using program edit checks, data listings review, medical review, quality review and source data verification. This could include reconciliation with external data.
- Data coding process to allow coding medical data received via the medical database per defined coding guidelines; this will include auto encoding and manual encoding process as well as coding reports review.
- Safety Event Database Reconciliation process to reconcile key safety event data variables stored in the Study clinical database and in the safety/pharmacovigilance database.
- Data review (interim, final) where quality of the data is evaluated, and general decisions are taken to ensure the data transmitted for the analysis will have the appropriate level of quality.
- Database lock and unlock process for interim and final Study database to restrict access to the database to avoid non-authorised modification of the clean database before the analyses. This includes extraction of the database in a specific location ensuring proper read only access but also no

change happened between the copy of extracted files and the removal of access rights of the database.

- Data transfer process (import and export) including development of transfer specifications to ensure transfers are performed according to specifications with appropriate quality check. Specification may include transfer method, format, frequency, content of the files (names/labels/formats of the variables), test transfer modality, detection of identifiable data including how they will be handled and specific measures to guarantee the security of the transfer of these data.

Data Management class of services may include Data Engineering (processing data to enable machine to machine data transmission for instance), Data Science (development of processing algorithms based on Artificial Intelligence techniques) and Data Analysis (restitution of data in a way adapted to their interpretation and support for decision making). A CRO with the appropriate expertise may also offer Data Anonymisation of Personal Data of Study Subjects via secure methods.

Subject matter of processing:	Establishing and/or following the established rules for verification of data accuracy, verification, data coding, data entry, communication for service delivery.
Purpose of the processing:	Verification, control, restoration of data accuracy.
Nature of the processing:	Collection/obtainment, access, analysis, alteration, combining, transfer/transmission, de-identification (pseudonymisation, anonymisation, aggregation, masking, removal of data elements), deletion/destruction, storage.
Types of Personal Data:	Study Subjects: health data, subject identification code, demographic data.
Duration of the processing:	Setup of Study database to database lock/transfer of trial master file, including anonymisation of all or part of Personal Data.

(10) Statistical analysis

Refers to the following activities:

- Development of a Statistical Analysis Plan (SAP) that describes the variables to be analysed and the method to be used to perform the analysis.
- Processes for statistical analyses covering the programming, quality control and delivery of statistical analysis, including the datasets, and statistical Tables, Figures and Listings (TFL) outputs and the process to communicate (where, how, access restricted) the results of the statistical analyses to the medical writer for the development of the CSR or any other stakeholders, e.g., Sponsor.

Subject matter of processing:	Analysis of Clinical Study Data obtained from the results of data management activities, communication for service delivery.
Purpose of the processing:	Statistical analyses of Study, development of TFLs.
Nature of the processing:	Collection/obtainment, analysis, combining, alteration, transfer/transmission, de-identification (pseudonymisation, anonymisation, aggregation, masking, removal of data elements), storage.
Types of Personal Data:	Study Subjects: health data, subject identification code, demographic data.
Duration of the processing:	SAP development to provision of CSR to Sponsor.

(11) Clinical Study Report (CSR)

Refers to all activities carried out to design the CSR that accurately reports the Study objectives, methods, the statistical analyses performed and their results.

The results are presented in an aggregated way, but some individual coded data can be listed as necessary.

Subject matter of processing:	Interpretation of Clinical Study Data in accordance with Study results, including aggregated and pseudonymous Personal Data.
Purpose of the processing:	Development of description, summary, presentation of analysis of the research via the CSR.
Nature of the processing:	Collection/obtainment, storage, alteration, transfer/transmission, deletion/destruction, de-identification (pseudonymisation, anonymisation, aggregation, masking, removal of data elements).
Types of Personal Data:	Study Subjects: health data, subject identification code, demographic data. Healthcare Professionals: name, position, place of work, opinions, qualifications, experience in clinical research, etc.
Duration of the processing:	Receipt of statistical analyses outcomes to acceptance of CSR by Sponsor.

(12) Financial management

Refers to all processes performed in the frame of the financial monitoring of a Clinical Study, and in particular the payment of Investigational Sites: fees and complementary procedures (additional examinations, products etc.).

Subject matter of processing:	Arrangement of money transfer, receipt of payment confirmations.
Purpose of the processing:	Execution of financial contractual obligations.
Nature of the processing:	Collection/obtainment, transfer/transmission, storage, deletion/destruction, de-identification (pseudonymisation, anonymisation, aggregation, masking, removal of data elements).
Types of Personal Data:	Healthcare Professionals: bank account numbers, contact details, location, position, etc.
Duration of the processing:	End of archiving period for financial accountability.

(13) Public disclosure

The public disclosure is the process where the results of statistical analyses outcomes, documentation developed for the Study, and CSR are spread in the public domain in various ways, such as regulatory agencies who made available the CSR to the public, or the Sponsor publishing the information in scientific journals or events.

Subject matter of processing:	Transfer of Clinical Study Data to a third-party location with subsequent disclosure by the third party.
Purpose of the processing:	Mandatory and requested/voluntary disclosure.
Nature of the processing:	Transfer/transmission (as disclosure methods), de-identification (pseudonymisation, anonymisation, aggregation, masking, removal of data elements), storage, deletion/destruction.
Types of Personal Data:	Study Subjects: health and demographic data[26]. Healthcare Professionals: name, position, place of work, opinions, qualifications, experience in clinical research, etc.
Duration of the processing:	Receipt of statistical analysis outcome/CRS to confirmation of performed disclosure.

[26] In rare cases the subject identification codes may be included in the publicly disclosed data sets, for example where there may be regulatory requirements to do so. This is not considered part of the ordinary course of events for this Class of Service, and therefore has been omitted. Where there is a necessity to include the subject identification codes, the CRO should receive from the controller a justification and document the necessity.

(14) Translation of Study documents/data

Refers to all activities carried out by the CRO for the translation of Study documents/data including Personal Data, e.g., CSR.

Subject matter of processing:	Change of the language code for the representation of Clinical Study Data.
Purpose of the processing:	Presentation of Clinical Study Data, including Personal Data, in the language understandable for the authorised recipients.
Nature of the processing:	Collection/obtainment, storage, de-identification (pseudonymisation, anonymisation, aggregation, masking, removing of data elements), translation, deletion/destruction.
Types of Personal Data:	Study Subjects: same as (4) Data collection, (8) Direct-to-patient services. Healthcare Professionals: same as (3) Site selection and contract.
Duration of the processing:	Delivery of the service, and partial archiving as required for Study purposes.

(15) Audits

Refers to all activities performed by a CRO in the frame of audits, e.g., on-site audits, commissioned where access to confidential information may be required for the audits where Personal Data falling under the scope of this Code may be concerned.

Subject matter of processing:	Review of Clinical Study Data and development of audit evidence.
Purpose of the processing:	Verification of legal, contractual, applicable standard/regulatory compliance.
Nature of the processing:	Collection/obtainment, analysis, transfer/transmission, storage, de-identification (pseudonymisation, anonymisation, aggregation, masking, removing of data elements), deletion/destruction.
Types of Personal Data:	Any Clinical Study Data, including Personal Data listed in all classes of services. Target data depend on audit scope.
Duration of the processing:	Audit request and preparation to end of archival period for the audit documentation, as required by applicable national law.

(16) Provision of IT managed services

Refers to the process of delivering all administration and management services required to maintain a software solution fully operational according to the terms of the Service Contract to a client. The owner of the source and executable code of the software solution can be a third party, as well as the provider of the IT infrastructure.

The applicable usage license conditions shall be included as part of the Service Contract, as well as all conditions of delivery of the software maintenance.

Such software license can be purchased directly by the Sponsor from the IT vendor and used by other CROs according to their Service Contract or purchased by the CRO from the IT vendor who then shall be listed in the sub-processors' list.

Examples of such IT platforms are the following:

- Electronic Data Capture system that can be accessed by Investigational Sites, CROs staff in charge of monitoring and / or data management as well as Sponsor's mandated staff.
- Clinical Trial Management System (CTMS).
- An Interactive Web Response System (IWRS) platform.
- An electronic Patient Reported Outcome (ePRO) platform etc.

Subject matter of processing:	Establishing tools/mechanisms to perform programmed data flow/processing.
Purpose of the processing:	Maintaining integrity, availability and confidentiality of data when processed through the delivered software solution.
Nature of the processing:	Collection/obtainment, storage, deletion/destruction.
Types of Personal Data:	Study Subjects: same as (4) Data collection, (8) Direct-to-Patient services. Healthcare Professionals: same as (3) site selection and contract.
Duration of the processing:	Until termination of consultation and maintenance.

(17) Provision of physical hosting infrastructure

Refers to all processes required to deliver to a client the necessary physical resources to host a software solution, such as secure data centre facilities, including processing capacity, data storage space, internet connectivity, monitoring systems etc. As well as possible virtualisation technologies and/or management resources.

Such services are to a large extent 'domain agnostic', and physical infrastructure can be implemented 'on premises' by a corporation or a hospital. However, continuity of service, security and confidentiality challenges are such, that the demand for the provision of Infrastructure as a Service or "virtualised data centre services" is growing and some countries throughout the EU member states have now developed standards (largely based on ISO 27001) or even certification processes for the delivery of such services when they are purchased for the delivery of IT solutions hosting health data. Where such services are supplied, they must be performed with suitable safeguards in place to protect the confidentiality, integrity, and availability of the data.

For the avoidance of doubt, this class of service is limited to the CRO acting as the data host and situations where it subcontracts the hosting and maintenance of the data are not included in this class of service.

Where this service is provided from a Third Country it is important to note that the Code requirements for international transfers must be met, and due consideration given to the location of both the processing facilities and the administrators who may remotely access the data.

Example:

A Sponsor purchases from an IT vendor an EDC-CTMS solution to run all its studies. The Service Contract foresees that the IT vendor provides a "turn-key" solution, with all the required secure hosting facilities (data centre, servers, firewall etc.).

If the software was provided on an "on-premises" mode, the secure hosting facilities would be those of the Sponsor and the secure hosting service would not be included neither in the Service Contract, nor in the related Data Processing Agreement.

Subject matter of processing:	Establishing and maintaining secure environment for data use.
Purpose of the processing:	Ensuring appropriate technical and organisational measures for data use.
Nature of the processing:	Collection/obtainment, storage, transfer/transmission, deletion/destruction.
Types of Personal Data:	Study Subjects: same as (4) Data collection, (8) Direct-to-patient services. Healthcare Professionals: same as (3) Site selection and contract.
Duration of the processing:	Until termination of service.

(18) User / Technical Support & Hotline

Refers to the process consisting of providing technical support to users of an IT platform used in the context of one or several Clinical Studies. This kind of service is usually included in the Service Contract of IT vendors. It can include a shared information system to record and follow every request for support (ticketing

system). It requires that Personal Data from the potential users (Investigators, clinical research assistants, clinical nurses etc.) be collected.

Because the users may refer to practical cases / situations, Study Subjects' data may be exchanged with the hotliners. This may also be the case if the IT platform includes ePRO or eCOA systems and first level support is provided by the IT vendor.

Subject matter of processing:	Providing technical support to resolve technical difficulties related to the use of software employed to process Personal Data.
Purpose of the processing:	Ensuring organisational security measures for data use, ensuring accuracy and availability of data.
Nature of the processing:	Collection/obtainment, storage, transfer/transmission, deletion/destruction, de-identification (pseudonymisation, anonymisation, aggregation, masking, removing of data elements).
Types of Personal Data:	Study subjects: same as (4) Data collection, (8) Direct-to-patient services. Healthcare professionals: same as (3) Site selection and contract.
Duration of the processing:	Until termination of service.

(19) Decommissioning services

Refers to the process consisting in removing / deleting all data of a client from the IT environment of the provider when the contractual relationship terminates.

The Service Contract shall include provisions for decommissioning services.

Decommissioning services shall be required for any class of services that envisages the employment of a computer system processing Personal Data.

The Data Processing Agreement shall implement the corresponding requirements for those data falling under the GDPR.

Example 1:

In this example, a Sponsor subcontracts the realisation of a Clinical Study to a CRO who purchases an EDC system for that specific Study. The EDC system is a multitenant system delivered as a Software as a Service (SaaS).

When the contract between the CRO and the IT Vendor terminates, decommissioning services consist of deleting all Clinical Study Data from the EDC platform. In this case through, the multitenant EDC software remains fully operational for other Studies after the decommissioning was completed.

Example 2:

In this example, a Sponsor purchases an EDC-CTMS system from an IT Vendor to carry a range of Clinical Studies. The EDC-CTMS system is required to be deployed in a dedicated secure hosting environment provided by the IT Vendor.

When the contract between the CRO and the IT Vendor terminates, decommissioning services consist of deleting the dedicated hosting environment, including Clinical Study Data from all the studies that have been performed using this EDC-CTMS platform.

Subject matter of processing:	Removing the concerned Personal Data from IT environment.
Purpose of the processing:	Securely removing all Personal Data from hosting environment.
Nature of the processing:	Deletion/destruction.
Types of Personal Data:	Study Subjects: same as (4) Data collection, (8) Direct-to-patient services. Healthcare Professionals: same as (3) Site selection and contract.

Duration of the processing:	Until termination/completion of service.

(20) Maintenance of Trial Master File (TMF)

TMF is set of electronic records and/or hardcopies relating to a Clinical Study, systematised and indexed for easy retrieval and use. The service consists of:

- Setup in agreement with the Sponsor's requirements, if any,
- Assigning responsibilities for the filing and maintenance;
- Identifying the Study documents that are subject to filing;
- Carrying out ongoing submission and processing of the documents,
- Storage;
- Review for accuracy and compliance with the regulatory and Sponsor's specifications; and
- Transfer to the Sponsor.

Subject matter of processing:	Data collection in accessible format with active access to data.
Purpose of the processing:	Essential Study documents, including Personal Data are catalogued in a standard manner, in compliance with ICH GCP and all other applicable standard.
Nature of the processing:	Collection/obtainment, storage, deletion/destruction.
Types of Personal Data:	Study Subjects: any pseudonymised Personal Data processed for the Research. Healthcare Professionals: any Personal Data processed for the Research.
Duration of the processing:	TMF setup to transmission of the TMF to the Sponsor.

(21) Archiving Services

Refers to services provided by the CRO to support the Sponsors or the Investigational Sites to comply with their obligations after the end of the Study.

For example, according to GCP and CTR (2014/536), Sponsors and Investigational Sites are required to archive all Study related documents (TMF) and Clinical Study Data.

Subject matter of processing:	Data storage in accessible format with no active access envisaged.
Purpose of the processing:	Maintaining data availability for regulators, future studies, additional authorisation submissions.
Nature of the processing:	Collection/obtainment, archival, deletion/destruction, de-identification (pseudonymisation, anonymisation, aggregation, masking, removing of data elements).
Types of Personal Data:	Study Subjects: any pseudonymised Personal Data processed for the Research. Healthcare Professionals: any Personal Data processed for the Research.
Duration of the processing:	For the relevant data covered, at least 25 years after the end or cancellation of the Clinical Research pursuant to the Clinical Trials Regulation No 536/2014 or Medical Device Regulation No 745/2017 as applicable; or any other duration according to type of studies and per applicable legal/regulatory/standard/contractual requirements.

(22) Regulatory/Study start up Services

Subject matter of processing:	Transfer of Personal Data to regulatory authorities for evaluation of Study personnel qualifications as a criterion of permission for Study conduct.
Purpose of the processing:	Compliance with the legal obligations to ensure appropriate qualifications of Healthcare Professionals through submission of regulatory dossiers accounting for adequate qualification of researchers/Investigators.
Nature of the processing:	Collection/obtainment, transfer/transmission, storage, archival, deletion/destruction.
Types of Personal Data:	Healthcare Professionals: surname, name, gender, date of birth, postal address, electronic and telephone contact details, bank details; education: qualification(s); professional life (including professional background, method and type of practice, necessary elements for assessing the knowledge they have for conducting the research); where applicable, registration number in the shared register of Healthcare Professionals; total compensation and remuneration received; participation in other studies, signature.
Duration of the processing:	As in (21) Archiving services.

(23) Arrangement of Investigator meetings

Subject matter of processing:	Collection and transfer of Personal Data of Healthcare Professionals to travel agencies, hotels, visa centres, and other third parties whose services are needed to enable transportation of Healthcare Professionals to the location of the Investigator meeting.
Purpose of the processing:	Ensure appropriate awareness of the Investigative team of the research protocol and Study requirements through delivering face to face research documents-focused trainings, enabling healthcare professional to network exchanging their experience in similar Research; especially relevant for multinational Research conducted at multiple Investigational Sites.
Nature of the processing:	Collection/obtainment, transfer/transmission, storage, de-identification (pseudonymisation, anonymisation, aggregation, masking, removing of data elements), deletion/destruction.
Types of Personal Data:	Healthcare Professionals: surname, name, postal address, electronic and telephone contact details, bank details; position, birth country, birth city, national ID type, national ID, citizenship status, citizenship country, nationality, travel details, national and international passport, visa applications, visa details, travel dates, itinerary, hotel booking details; bank account numbers, etc.
Duration of the processing:	From acceptance by Healthcare Professional of the invitation to the Investigator meeting to the provision of compensation of travel expenses to the Healthcare Professional by the Sponsor; and/or end of retention of all financial accountability documents by CRO.

Appendix 3 - Declaration of direct or indirect interests

Complements section 5.2.5 "Conflicts of Interests" (at the level of the Monitoring Body)

DECLARATION OF INTERESTS

I, the undersigned, ……

Acknowledge being aware of the obligation to declare all interests, be they direct or via an intermediary, with:

1 CROs which are members or non-members of EUCROF, as defined in paragraph 1.1 “Terminology” of the Code of Conduct and the activities of which fall within the scope of application set out in paragraph 1.4 “Scope of Application” of this Code of Conduct (hereinafter referred to as “**CROs**”);

2 and the businesses, establishments, or organisations—including consultancy firms, audit firms, and professional bodies—the activities, technologies, and products of which fall under the jurisdiction of CROs.

I am completing this declaration in the capacity of:

- ☐ A member of the Supervisory Committee (COSUP)
- ☐ Chair of the Supervisory Committee (COSUP)
- ☐ Vice Chair of the Supervisory Committee (COSUP)

I undertake to update my declaration of interests as soon a change occurs regarding these interests or new interests arise, and at minimum annually even if there is no such change.

It is your responsibility, upon receiving the agenda of a meeting, to check whether the interests you have declared or which could arise on an ad-hoc basis are compatible with your presence at all or part of that meeting and to notify the designated contact person within COSUP and, if applicable, the Chair of the meeting, of such, if possible before it is held.

In the event of conflicts of interest, your presence could give rise to irregularities in the decisions made or recommendations, references, or opinions issued and cause the decision made, or that which COSUP could have made based upon said deliberation, to be rendered void.

1. Your main occupation

1.1. Current main occupation (remunerated or not)

Professional occupation:

OCCUPATION/ ROLE	**NATURE OF WORK** *(Employment/Contract/Voluntary)*	**EMPLOYER / CLIENT / ORGANISATION**	**LOCATION**	**START** *(month/year)*	**END** *(month/year)*

1.2. Occupations undertaken as a main occupation during the last three years (remunerated or not)

Other than those entered in section 1.1

Professional occupation:

OCCUPATION/ ROLE	**NATURE OF WORK** *(Employment/Contract/Voluntary)*	**EMPLOYER / CLIENT / ORGANISATION**	**LOCATION**	**START** *(month/year)*	**END** *(month/year)*

2. Secondary occupations

2.1 List here your current or former participations in a decision-making body of a public or private organisation, the activity, technologies, or products of which fall within the jurisdiction of CROs.

In particular, this includes healthcare establishments, consultancy forms and bodies, professional bodies (learned societies, healthcare networks, the National Social Insurance), and patient associations.

- ❑ I have no interests to declare in this section.
- ❑ Currently or in the last three years:

ORGANISATION *(company, establishment, association)*	**Position** *in the organisation*	**REMUNERATION** *(amount to be indicated in table A1)*	**START** *(month/year)*	**END** *(month/year)*
		❑ None ❑ To the declarant ❑ To an organisation in which you are a member or employee *(please specify)* …….. ……		
		❑ None ❑ To the declarant ❑ To an organisation in which you are a member or employee *(please specify)* ……		

2.2 List here all current or former consultancy, advisory, or expert activities within a public or private body, the activity, technologies, or products of which fall under the jurisdiction of CROs.

Included in this section are advisory or representation activities, participation in a work ground or scientific council, audit activities, or writing expert reports.

- ❑ I have no interests to declare in this section.
- ❑ Currently or in the last three years:

ORGANISATION *(company, establishment, association)*	**TASKS /POSITION**	**REMUNERATION** *(amount to be indicated in table A2)*	**START** *(month/year)*	**END** *(month/year)*
		❑ None ❑ To the declarant ❑ To an organisation in which you are a member or employee *(please specify)* …… ……...		

ORGANISATION *(company, establishment, association)*	**TASKS /POSITION**	**REMUNERATION** *(amount to be indicated in table A2)*	**START** *(month/year)*	**END** *(month/year)*
		❑ None ❑ To the declarant ❑ To an organisation in which you are a member or employee *(please specify)* …… ……		

2.3 List here all current or former participations in scientific works and studies for a public or private body, the activity, technologies, or products of which fall under the jurisdiction of CROs.

Participation in scientific works and the performance of clinical or preclinical trial or studies, epidemiological studies, medico-economic studies, observational studies, etc. must be mentioned.

The position of member of a monitoring and follow-up committee of a clinical Study must be declared in this section.

- ❑ I have no interests to declare in this section.
- ❑ Currently or in the last three years:

Sponsoring Organisation *(company, establishment, association)*	**Financing organisation** *(if different to the Sponsor and if you know it)*	**Subject** *(name of Study, product, technique, or therapeutic indication)*	**REMUNERATION** *(amount to be indicated in table A.3)*	**START** *(month/year)*	**END** *(month/year)*
			❑ None ❑ To the declarant ❑ To an organisation in which you are a member or employee *(please specify)* …… ……		
			❑ None ❑ To the declarant ❑ To an organisation in which you are a member or employee *(please specify)* …… ……		

2.4 List here all articles, speeches at congresses, conferences, colloquia, various public meetings or training organized or financially supported by businesses or public or private bodies, the activity, technologies, or products of which fall under the jurisdiction of CROs.

The writing of article and talks must be declared when they were remunerated or gave rise to compensation.

- ❑ I have no interests to declare in this section.
- ❑ Currently or in the last three years:

Business or organisation *(company, association)*	**For speeches, place and title of event**	**Topic** of the article or talk and name of the target product if applicable	**Compensation for travel costs**	**Remuneration** *(amount to be indicated in table A.4)*	**START** *(month/year)*	**END** *(month/year)*
			❑ Yes ❑ No	❑ None ❑ To the declarant ❑ To an organisation in which you are a member or employee *(please specify)* ……..		
			❑ Yes ❑ No	❑ None ❑ To the declarant ❑ To an organisation of which you are a member or employee *(please specify)* ……		

2.5 List here your current or past activities as an inventor and/or the owner of a patent or a product, process, or any other form of non-patented intellectual property relevant to the jurisdiction of CROs.

- ❑ I have no interests to declare in this section.
- ❑ Currently or in the last three years:

Nature of activity *and name of patent, product, etc.*	**Body** *providing the patent, product, etc.*	**Revenue / profit sharing**	**Remuneration** *(amount to be indicated in table A.5)*	**START** *(month/year)*	**END** *(month/year)*
		❑ Yes ❑ No	❑ None ❑ To the declarant ❑ To an organisation in which you are a member or employee *(please specify)* ……..		
		❑ Yes ❑ No	❑ None ❑ To the declarant ❑ To an organisation in which you are a member or employee *(please specify)* ……..		

3. Activities that you lead or have led and which benefited from financing from a for-profit organisation whose corporate purpose falls within the jurisdiction of CROs.

The type of payment can take the form of subsidies or contracts for studies or materials, grants or sponsorship, monetary or in-kind payments, equipment, apprenticeship tax, etc.

This includes chairs, treasurers, and members of offices and executive boards, including associations and learned society.

- ❑ I have no interests to declare in this section.
- ❑ Currently or in the last three years:

BODY AND ACTIVITY Beneficiaries of financing	**For-profit ORGANISATION(s) (*)**	**START** *(month/year)*	**END** (month/year)

(*) The amount paid by the financer(s) with optional indication of the percentage of the amount of the financing in relation to the budget of the body shall be indicated in table B.1.

4. Financial participation in the capital of a company, the corporate purpose of which falls within the jurisdiction of CROs.

Financial participations in the form of listed or unlisted transferable securities, whether shares, bonds, or other financial assets in equity in a relevant business or sector, one of its subsidiaries or a company of which it holds a part of the capital to the extent of your immediate and expected knowledge must be declared.

It is required that you state the name of the establishment, business, or organisation, the type of financial participations, and their amount as an absolute value and as a percentage of the capital held.

(Open-end trust- or unit trust-type investment funds in collective products—of which the person controls neither the management nor the composition—are excluded from the declaration).

- ❑ I have no interests to declare in this section.
- ❑ Currently or in the last three years:

RELEVANT BODY	**TYPE OF INVESTMENT (*)**

(*) The percentage of the investment in the capital of the body and the amount held shall be indicated in table C.1.

5. Close relatives with activities or financial interests in any body whose corporate purpose falls within the jurisdiction of CROs.

Concerned people are:
- *your partner (spouse, common-law partner, or civil-law partner), as well as the parents (father and mother) and child(ren) of the latter;*
- *your children;*
- *your parents (father and mother).*

In this section, you must declare if you are aware:
- *of any occupations (within the meaning of section 1 to 3 of this document) performed or led or during the past 3 years by your close relatives*
- *of any direct financial participation in the capital of a company (within the meaning of section 4 of this document) above an amount of 5,000 euros or 5% of the capital held by your close relatives.*

You must identify the relevant third party by your relationship only.

- ❑ I have no interests to declare in this section.
- ❑ Currently or in the last three years:

Close relative(s) with a connection to the following organisations *(The relationship shall be indicated in table D.1.)*	**RELEVANT ORGANISATIONS**	**Occupations (current or within the past 5 years)**	**Shareholding** *Current direct financial participation above an amount of 5,000 euros or 5% of the capital (The amount shall be indicated in the table)*

Close relative(s) with a connection to the following organisations *(The relationship shall be indicated in table D.1.)*	**RELEVANT ORGANISATIONS**	**Occupations (current or within the past 5 years)**	**Shareholding** *Current direct financial participation above an amount of 5,000 euros or 5% of the capital (The amount shall be indicated in the table)*

6. Other interests that you think shall be brought to COSUP's attention

- ❑ I have no interests to declare in this section.
- ❑ Currently or in the last three years:

RELEVANT ITEM OR FACT	**COMMENTS** *(the amount of the sums received shall be indicated in table E.1.)*	**Start YEAR**	**End YEAR**

7. If you have entered no information after 1, check the box and sign the last page ❑

[TO BE COMPLETED if applicable: you may be sanctioned for having knowingly neglected to fill out or amend a declaration of interest in order to update the data therein or providing misleading information which infringes the honesty of this declaration]

8. Tables of particulars not to be disclosed

Table A.1

ORGANISATION	**AMOUNT RECEIVED**

Table A.2

ORGANISATION	**AMOUNT RECEIVED**

Table A.3

ORGANISATION	**AMOUNT RECEIVED**

Table A.4

BUSINESS or ORGANISATION	**AMOUNT RECEIVED**

Table A.5

BODY	**AMOUNT RECEIVED**

Table B.1

ORGANISATION	**Percentage of amount received** from financing in relation to the operating budget of the body and the amount paid by the financer

Table C.1

BODY	**Percentage** *of the investment in the capital of the body and the amount held*

Table D.1

	SALARIED	**SHAREHOLDER**			
Organisation	**Job position** *(State, if applicable, if it is a position with responsibilities)*	**Amount** *If ≥ EUR 5,000 or 5% of the capital*	**Relationship**	**Start** *(month/year)*	**End** *(month/year)*

Table E.1

RELEVANT ITEM OR FACT	**SPECIFY the amounts received if applicable**

Done in

on

Signature (mandatory)
(Particulars not to be disclosed)

EUCROF is the data controller with the purpose of preventing conflicts of interests by taking into consideration the interests declared thus declared on the agendas of meetings held by COSUP in keeping with the requirements of the Code of Conduct approved by the competent authorities in the area of the protection of Personal Data. The information collected on this form will be saved and published on the EUCROF website for the purposes of transparency, with the exception of the information in part 8.

This information will be kept for [TO BE COMPLETED] years from their transmission to EUCROF.

In accordance with the French Data Protection Act and the European Data Protection Regulation, you may exercise your right to access data about you and have them rectified by contacting the head of data protection at EUCROF at the following address [TO BE COMPLETED]. You also have the right to the deletion and restriction of your data, as well as the right to make a claim before the French Data Protection Authority (CNIL).

You may also specify instructions regarding what shall be done with your Personal Data after your death by contacting the head of data protection at EUCROF directly for specific instructions, or to any third-party digital confidence provider certified by CNIL and registered in the unique register, the methods and access of which will be set by decree of the State Council for General Directives.

The contact details of the EUCROF data protection officer are as follows: [TO BE COMPLETED]

Appendix 4 - Engagement of independence and confidentiality

Complements section 5.2.5 "Conflicts of Interests" (at the level of the Monitoring Body)

APPENDIX 5

COMMITMENT AND CONFIDENTIALITY MODEL

I, the undersigned, ……

make the following commitments of independence and confidentiality in the context of my appointment to my position:

- ☐ A member of the Supervisory Committee (COSUP)
- ☐ Chair of the Supervisory Committee (COSUP)
- ☐ Vice Chair of the Supervisory Committee (COSUP)

Independence

I undertake to fulfil my mandate within COSUP in complete independence and to not submit to pressure that could influence my behaviour in the exercise of my mandate.

In particular, I undertake to systematically verify before every meeting whether the interests that I have declared (see Appendix 4 of the Code of Conduct) or that could arise on an ad-hoc basis are compatible with my presence during all or part of said meeting.

Failing that I undertake to warn the designated contact person within COSUP of such and, if applicable, the Chair of the meeting, if possible before it is held.

I undertake to withdraw from the meeting in the event of conflicts of interest, as my presence could give rise to irregularities in the decisions made or recommendations, references or opinions issues and cause the decision made, or that which COSUP could have made based upon said deliberation, to be rendered void.

Confidentiality

I acknowledge that all facts, acts, and information to which I have direct or indirect access in the exercise of my mandate, including not only that which has been told to me, but also that which I have seen, heard, or understood, are confidential information ("**Confidential Information**").

The obligation of confidentiality to which I am bound consists of not disclosing, by any means, the Confidential Information of which I learned during the exercise of my mandate both to members of EUCROF—save if they themselves are authorised know the Confidential Information in question—and to external persons.

That other persons are aware of the Confidential Information does not affect their confidential and secret character.

This obligation of confidentiality remains binding after the end of my mandate, regardless of its duration.

Done in ……. Signature

End of document