CRO GDPR Code of Conduct
What you should know…

EHDPC Conference

16 October 2024

EUCROF Code Task Force

GDPR: 6 years already!

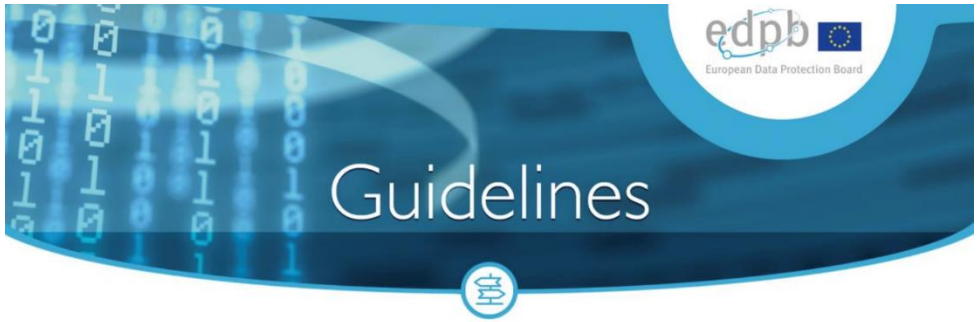
Special sector

Article 9: special categories of personal data.
The treatment of health data, genetic data …

Except…

Code of conduct & GDPR

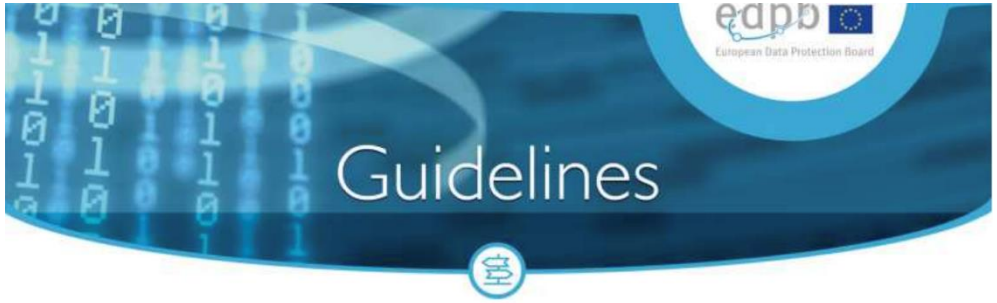
Art 40-41 GDPR



Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679

Version 2.0

4 June 2019



Guidelines 04/2021 on codes of conduct as tools for transfers

Adopted on 07 July 2021

Code of conduct vs certification

What is the Code

The 1st transnational GDPR code in the area of clinical research

6 years of continuous efforts of international team of professionals in clinical research, data protection, IT, auditing, etc…

It is the specific interpretation, approved by the supervisory authorities, of how the GDPR should be implemented for clinical research.

Approved since 12-SEP-2024

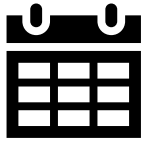
- European Data Protection Board (EDPB) have provided their favourable opinion (Opinion 12/2024) in June subject to final tweaks.

  https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-122024-draft-decision-french-supervisory_en

- CNIL formally approve in their September plenary (Decision 2024-064).

  https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000050248562?init=true&page=1&query=&searchField=ALL&tab_selection=cnil&timeInterval=

- Download from https://cro.eucrof.eu/gdpr-form
- Now: recruiting members of the Monitoring Body (info@eucrof.eu)
- Accreditation (COSUP) and first adherence: Q1 2025



What is the Code?

- **European CRO Federation developed a task force to write a GDPR Code that would apply to CROs.**
- **Task force has had multi-stakeholder input.**

What is the Code

- **Who is covered?**

  Service Providers for clinical research acting as a **Data Processor** for the research/study sponsor in the frame of a **Service Contract**

  Service Providers are full-service CROs and specialised single-service vendors e.g., IT
- **What is covered?**

  23 classes of services that a CRO can deliver.
- **Whose data are covered?**

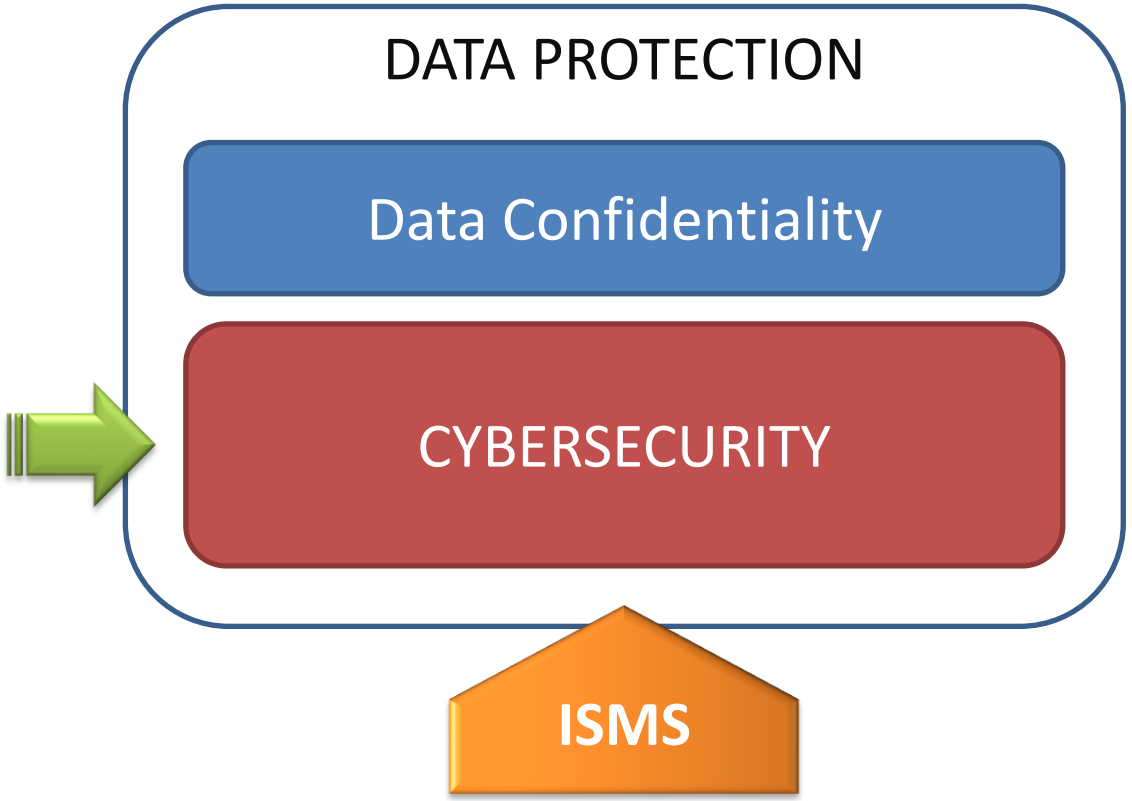
  Patients & healthcare professionals
- **What geographical area?**

  27 European Union Member States

What Is the Code and Why We Need It

Guarantees "state of the art" security & confidentiality management

… controller shall use **only processors providing sufficient guarantees** to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject



- More certainty about the sufficient nature of the guarantees required from subcontractors
- Adaptation of requirements to different types of subcontractors (as opposed to “one size fits all”)
- Harmonization at EU level
- Simplification of vendor assessments
- …

EUCROF European CRO Federation

The founding principle
Service contract

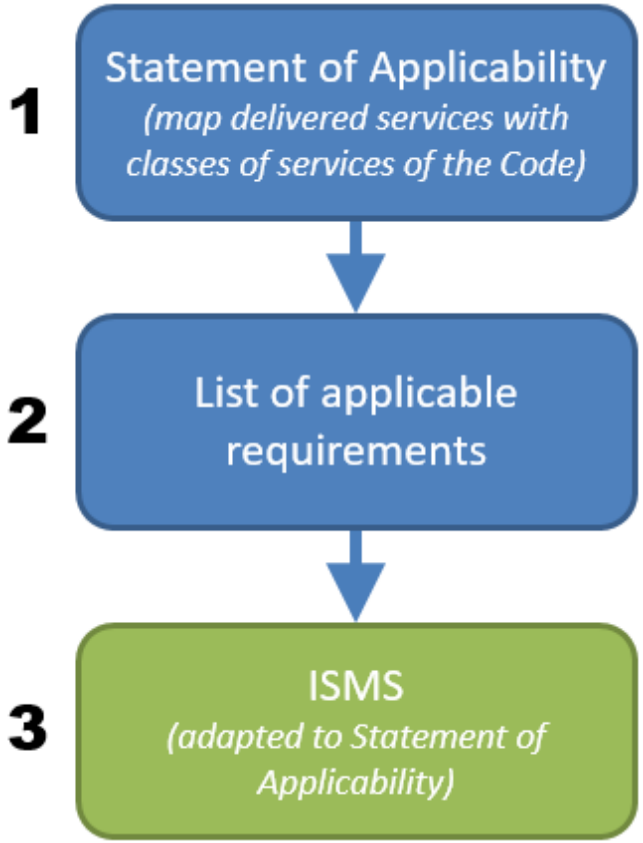
Pursuant to Article 82 "Right to compensation and liability" recital 2 of GDPR

[…] 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.

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 and the corresponding **Data Processing Agreement**

What the EUCROF Code is ?

Upgrade QMS with an ISMS



The vast majority of CROs, whatever their size, already have an ISO 9001:2015 certified Quality Management System…

Methods of compliance specific to the CRO shall be appropriately documented and monitored by means of "records".

This shall be realised by means of an **ISMS – Information Security Management System** based on ISO 9001, ISO 27001 and ISO 27701 standards

What Is the Code

Security + Transparency : build trust and confidence

Public registry

https://cro.eucrof.eu/eucrof-code-public-registry

A tool to foster transparency towards patients, investigational sites, pharma, biotechs, medtechs, ethics committees, authorities …

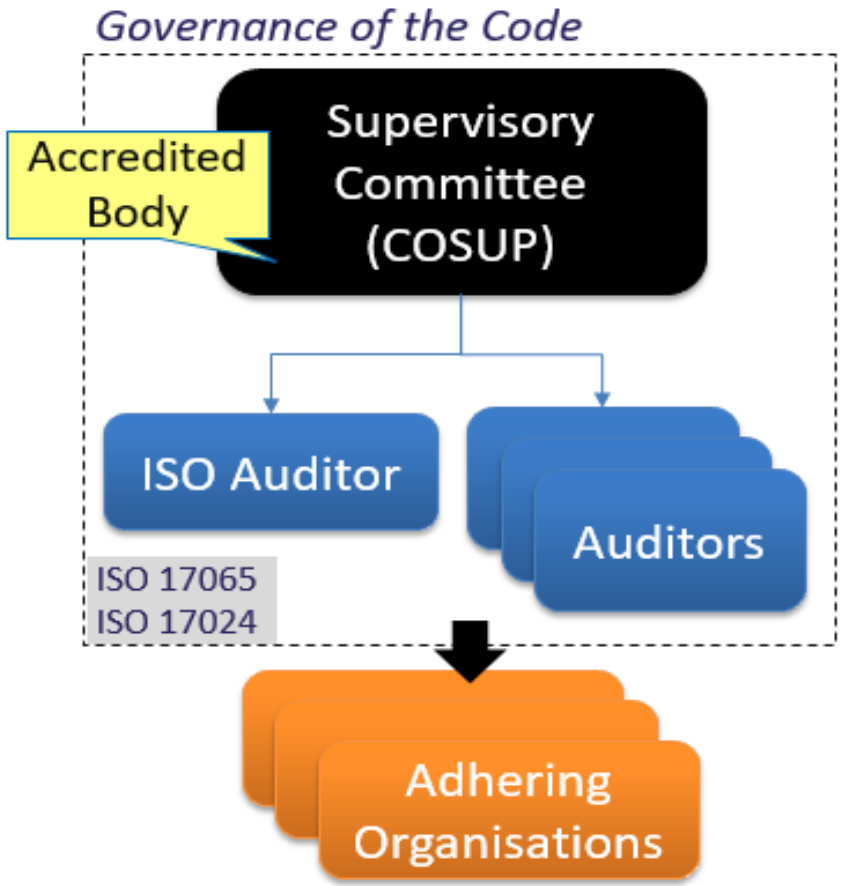
Reduce the burden of audits and vendor assessments
in an harmonized EU landscape

Any "service provider" - EUCROF affiliate or not

EUCROF
European CRO Federation

What Is the Code and How It Works

An accredited "control body"



- EUCROF is the owner of the Code
- An Internal Monitoring Body (COSUP)
- Independence, impartiality

- Now: recruiting members of the Monitoring Body (info@eucrof.eu)
- Accreditation (COSUP) early Q1 2025

What the Code is NOT

- NOT a tool for international data transfers
- NOT about processing by CROs as data controllers
- NOT about GDPR compliance responsibilities of sponsors and sites

Why we need the Code

Adhering CROs

- Reduce administrative and operational waste.
- Obtain practical guidance on showing and keeping GDPR compliance.
- Align approaches with other adhering members, select sub-contractors / partners.
- Display Compliance Mark as sign of high standard study services.

Investigational sites

- Streamline GDPR compliance / acceptance of compliant CROs / Vendors.
- Rely on list of Code adhering CROs when assessing reliable CROs.

Sponsors contracting adhering CROs

- The same acknowledged "compliance scheme" in all 27 EU Member States.
- Reduce expenses into data protection audits of vendors.
- Easy (online) access to compliance records of selected CROs / Vendors.

What does compliance with the Code look like?

- CROs who are adherent to the Code have to apply to the monitoring body of the Code to have their compliance reviewed / audited.
- No CRO who has not been through the adherence process will be able to display the EUCROF Code of Conduct Compliance Mark.
- Only companies who are listed on the Public Registry are CRO adherents.

What does compliance with the Code look like?

Models

Level 1: Declarative adherence

Simplified submission, review of submitted policies

- CRO completes an organizational profile and a compliance questionnaire.
- Code's Supervisory Body (COSUP) reviews the compliance dossier.
- COSUP issue resolution on evaluation and grants Compliance Mark to successful CROs.

Level 2: Third party assessment

Higher complexity, review of available policies and evaluation of implemented processes

- CRO completes compliance dossier as step 1.
- Eligible candidate CRO undergoes an on-site audit by one or more COSUP Auditors.
- Auditors report audit findings to the COSUP.
- COSUP gives final decision on the candidate CRO and grants Compliance Mark to successful CROs.

Practical implementation guidance

Overview

- Compliance Model
  - The Code has requirements throughout – each is numbered.
  - The Code describes 23 services that a CRO might provide.
  - A matrix indicates which requirements apply to each service.
- Statement of Applicability
  - CRO will have the responsibility to define which of its services it wishes to accredit.
  - This will mean each CRO will have its own statement of applicability which lists what requirements of the Code they must adhere to. This is an individual CRO's compliance framework.

Practical implementation guidance

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.

Practical implementation guidance

Classes of Services

(to be extended in the following Code versions)

(1) Synopsis, protocol and CRF design
(2) ICF design & information leaflet
(3) Site selection and contract
(4) Data collection
(5) Monitoring
(6) Medical monitoring
(7) Pharmacovigilance (PVG) and safety reporting
(8) Direct-to-Patient (DtP) services
(9) Data management
(10) Statistical analysis
(11) Clinical Study Report (CSR)
(12) Financial management
(13) Public disclosure
(14) Translation of study documents/data
(15) Audits
(16) IT-managed services
(17) Provision of physical infrastructure
(18) User / Technical support & hotline
(19) Decommissioning services
(20) Maintenance of Trial Master File
(21) Archiving Services
(22) Regulatory / Study start-up services
(23) Arrangement of Investigator Meetings

Practical implementation guidance

Definition of Class of Services

(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:	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.

Practical implementation guidance

Overview of Compliance Areas in the Code

Contracts	Principles	Compliance Activities	Security
Contents of Contracts e.g., • Client and Vendor service agreements • Transfer information	Rules for implementing Principles e.g., • Data minimisation • Storage limitation • Purpose limitation • Transparency • Confidentiality	Activities CROs must perform e.g., • Management of vendors • DPO appointment • Transfer formalities • Breach notification	• Technical and organisational measures required to secure data according to risk of service/data e.g., adopt ISO 27001 controls as per matrix

EUCROF European CRO Federation

How to apply

Overview of Adherence Process

1. Any "Service Provider" in scope of the Code (EUCROF Affiliate or not)
2. An online process (https://cro.eucrof.eu/) to check compliance and submit compliance file & apply for review by COSUP
3. Review by COSUP
4. Approval by COSUP of compliance dossier: CRO listed on Public Registry with compliance mark level 1 "declarative adherence", with possibility to escalate to level 2
5. If Level 2 is selected, COSUP allocates one or more Auditors
6. Onsite audit of the CRO & audit report generated
7. Review of audit report by Auditor, RCO with the COSUP
8. Approval by COSUP: listed on Public Registry with compliance mark level 2 “third party assessment”

How to apply

IT Platform has been created for an easy way to submit adherence file to the COSUP

Launch of 1st release of the online platform was in November 2021

Public Registry (https://cro.eucrof.eu/eucrof-code-public-registry)

- Lists all adherent CROs with corresponding compliance mark and Statement of Applicability (classes of services covered by their compliance mark)

Public access to the description of "classes of services"

- Allows benchmarking of what is covered by classes of services at https://cro.eucrof.eu/eucrof-code-classes-services

Private access for “CoC Supervisory Committee"

- Update public registry & public page of classes of services
- Authorise access to CRO Managers to engage submission of adherence file
- Update "classes of services", "requirements" and mapping matrix

CRO Managers

- Access online submission interface & follow-up
- User Manual for CRO Managers

EUCROF European CRO Federation

If you are interested in hearing more or participating in the Code scheme you can email info@eucrof.com

Thank you for your attention!