



D6.1. – Implementation of ethical standards and guidelines of H2020 and GDPR implementation plan

Related Work Package	WP6 – Regulatory, ethical and cost effectiveness aspects
Related Task	Task 6.1- Ethics and legal issues monitoring
Lead Beneficiary	UOI
Contributing Beneficiaries	ALL
Document version	v.1.0
Deliverable Type	Report
Distribution level	Public
Target Readers	All partners
Contractual Date of Delivery	31/12/2021
Actual Date of Delivery	01/01/2022

Authors	Michalis Mantzaris, Alexandros Mitsis
Contributors	ALL
Reviewer	Elisavet Papageorgiou



This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 945175



List of Contributing Beneficiaries

No	Organisation name	Short name	Country
1	PANEPISTIMIO IOANNINON	UOI	GREECE
2	ISTITUTO EUROPEO DI ONCOLOGIA SRL	IEO	ITALY
3	OGKOLOGIKO KENTRO TRAPEZAS KYPROU	BOCOC	CYPRUS
4	IDRYMA TECHNOLOGIAS KAI EREVNAS	FORTH	GREECE
5	I.M.S. - ISTITUTO DI MANAGEMENT SANITARIO SRL	IMS	ITALY
6	PHILIPS ELECTRONICS NEDERLAND BV	PHILIPS	NETHERLANDS
7	REGION STOCKHOLM (KSBC)	KSBC	SWEDEN
8	STREMBLE VENTURES LTD	STREMBLE	CYPRUS
9	ONKOLOSKI INSTITUT LJUBLJANA	IOL	SLOVENIA
10	ETHNIKO KAI KAPODISTRIAKO PANEPISTIMIO ATHINON	NKUA	GREECE
11	SOCIETE EUROPEENNE DE CARDIOLOGIE	ESC	FRANCE
12	ELLINIKO MESOGEIAKO PANEPISTIMIO	HMU	GREECE

Version history

Version	Description	Date completed
v0.1	Table of Contents (TOC) circulation M. Mantzaris (UOI)	01/12/2021
v0.2	First draft consolidation M. Mantzaris (UOI) A. Mitsis (UOI)	20/12/2021
v0.3	Review of the deliverable Elisavet Papageorgiou (BOCOC)	27/12/2021
v0.4	Review comments incorporated M. Mantzaris (UOI), A. Mitsis (UOI)	31/12/2021
v1.0	Final version submission	31/12/2021

Statement of Originality

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

Disclaimer

This document contains material, which is the copyright of one or more CARDIOCARE consortium parties, and may not be reproduced or copied without permission.

The commercial use of any information contained in this document may require a license from the proprietor of that information.

Neither the CARDIOCARE consortium as a whole, nor individual CARDIOCARE consortium parties, warrant that the information contained in this document is capable of use, nor that the use of the information is free from risk, accepting no liability for loss or damage suffered by any person using this information.

Compliance of Deliverable 6.1 with the Description of Action

DoA Task description	Addressed by D6.1
<p>Description of Action Task 6.1. Ethics and legal issues monitoring (pdf page 116)</p> <p>All ethical standards and guidelines of Horizon 2020 will be rigorously applied, regardless of the country in which the research is carried out. Medical research will comply with international and EU conventions, declarations and regulations.</p>	<ul style="list-style-type: none"> • Section 3. Ethical standards and guidelines of Horizon 2020, pages 10-13, addresses the ethical aspects of project activities • Section 5. CARDIOCARE compliance with ethical standards and guidelines, pages 16-18, provides project activities for ethical compliance
<p>The clinical study protocol will be sent for approval by the competent ethics committees</p>	<ul style="list-style-type: none"> • Section 1. Introduction, page 8, refers to Deliverable 1.1 which provides ethics approval status for each centre participating in the retrospective clinical study
<p>To ensure a Data Protection by Design strategy a GDPR implementation plan will be devised.</p>	<ul style="list-style-type: none"> • Section 5.3 GDPR implementation plan, pages 18-24, describes the plan implemented for GDPR compliance
<p>An ethical advisory board will be established for monitoring the compliance of the project’s activities with the legal, ethical, data protection, privacy and security aspects.</p>	<ul style="list-style-type: none"> • Section 4.1 Ethical Advisory Board (EAB), page 14, presents the board members and its role.



Executive summary

Deliverable D6.1 concerns the implementation of the **ethical standards and guidelines of Horizon 2020 that must be applied** by all beneficiaries and includes the **GDPR implementation plan** for the CARDIOCARE project.

CARDIOCARE is an interdisciplinary clinical research project. The project is an international collaboration of 12 institutions from 7 countries across Europe (Greece, Italy, Cyprus, Slovenia, Sweden, Netherlands, and France) aiming to improve the monitoring, treatment and overall care provided to the elderly breast cancer patients which are at higher risk of developing cardiac toxicity from cancer therapy. Already available retrospective data and data collected within a new prospective clinical study will be used for the development and validation of a novel Risk Stratification model for the elderly breast cancer patients.

The types of personal data that shall be shared for the research purposes of the project include clinical data, cardiac imaging, serum biomarkers and psycho-markers, multi-omics (genomics, epigenomics, metagenomics) data, Quality of Life data and intrinsic (mental and physical) capacity monitoring data including wearable sensor and mobile Health application data. Considering the special category/sensitive nature of the personal data that shall be processed, comprising health and genetic data, as well as the requirement to transfer such data to other CARDIOCARE partners for processing, raises several legal, ethical, privacy and security issues that must be managed by appropriate organisational and technical measures implemented in the CARDIOCARE project for the protection of the rights and freedoms of the data subjects.

To this end, all ethical standards and guidelines of Horizon 2020 will be rigorously applied, in all EU-based partners of the consortium, in which the research is carried out. Medical research will comply with international and EU conventions, declarations and regulations. Appropriate Informed Consent procedures will be followed in line with the GDPR emphasizing in the lawful, fair and transparent processing of the data based on the principles of data minimisation and purpose limitation. Special emphasis has been given in informing patients about i) the objectives of the project, ii) the legal basis for requesting/obtaining their data, iii) their rights and how to exercise them, (iv) methods used for collecting and processing their personal data, (v) duration of data use and storage, and (iv) appropriate privacy and data protection safeguards. To ensure that a Data Protection by Design strategy shall be implemented from the beginning of the project a GDPR implementation plan has been devised and presented in this deliverable.



Table of Contents

1	Introduction.....	8
2	Geographical distribution of the CARDIOCARE consortium.....	9
3	Ethical standards and guidelines of Horizon 2020	10
4	Ethics and legal issues monitoring	14
4.1	Ethical Advisory Board (EAB).....	14
4.2	Regulatory Advisory Board (RAB).....	15
5	CARDIOCARE compliance with ethical standards and guidelines	16
5.1	Informed Consent Procedures	16
5.1.1	Language and terms	17
5.1.2	Copies of the Informed Consent Forms, Information Sheets & Ethical Approvals	17
5.1.3	Incidental Findings Policy	17
5.1.4	Patient 'Profiling' involving tracking or observation of participants.....	17
5.2	Human cells / tissues obtained within the project.....	18
5.3	GDPR implementation plan.....	18
5.3.1	GDPR Scope	19
5.3.2	GDPR definitions.....	19
5.3.3	GDPR Principles	20
5.3.4	Data Protection by Design strategy.....	21
6	Conclusions.....	25
7	Appendix (Data Sharing Agreement, Privacy Notice & DPIA-UOI).....	26



List of Abbreviations

Abbreviation	Explanation
DMP	Data Management Plan
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EAB	Ethical Advisory Board
EEA	European Economic Area
FAIR	Findable Accessible Interoperable Re-usable
GDPR	General Data Protection regulation
ICO	Information Commissioner's Office
ICOS	International Cardio-Oncology Society
ORD	Open Research Data
RAB	Regulatory Advisory Board

List of Tables

Table 1: Relevant National legislation and guidelines.	11
Table 2: EAB members	14
Table 3: RAB members	15

List of Figures

Figure 1: Geographical distribution of the CARDIO CARE consortium.....	9
Figure 2: GDPR is applied in both EU and EEA countries.	19
Figure 3: Data categories, Roles, Data Sharing Agreement, and data transfers.....	24



1 Introduction

The information provided in this deliverable follows the ethical standards and guidelines of Horizon 2020 and the GDPR regulation ensuring that all ethical and legal aspects are addressed prior to the commencement of the related project activities. The deliverable provides information on:

- The geographical distribution of the CARDIOCARE consortium.
- The Ethical standards and guidelines of Horizon 2020.
- Ethics and legal issues monitoring.
- Project compliance with ethical standards and guidelines.
- GDPR implementation plan.

Additional information on the procedures for **data collection, storage, protection, retention, reuse and/or destruction** is provided in Deliverable D5.1 (Data Management Plan) which is considered a “living document” with clear version numbers in which information can be made available on a finer level of granularity through updates, as the implementation of the project progresses. In Deliverable D1.1, the **first study subject approval package for the retrospective study** is provided, including **ethical approval status** for each centre participating in the retrospective clinical study.

2 Geographical distribution of the CARDIO CARE consortium

CARDIO CARE consortium comprises 12 partners including, (i) six clinical centers (IEO, BOCOC, KSBC, UOI, NKUA, IOL), (ii) five technical partners of which a Research Institute (FORTH), two Universities (UOI, HMU) and three SMEs (PHILIPS, IMS, STREMBLE), and (iii) a medical association (ESC). The geographical distribution of the participating institutions includes seven **EU member states** (Italy, Greece, Netherlands, France, Sweden, Slovenia and Cyprus) as shown in **Fig.1**. Data sharing activities for the purposes of the project do not involve data transfers to non-EU member states.



Figure 1: Geographical distribution of the CARDIO CARE consortium.



3 Ethical standards and guidelines of Horizon 2020

The large amount of data collection from multiple sites across Europe, the different types and categories of data including personal and special category data and the transfer of such data for centralized analysis raise legal, ethical, privacy and security issues that have to be managed by appropriate organisational and technical measures implemented in the CARDIOCARE project.

To this end, all project activities performed for the collection, use, transfer and protection of data, including biological samples will follow the ethical standards and guidelines of Horizon 2020 including the Charter of Fundamental Rights of the European Union¹ and the European Convention on Human Rights². Patients' data and biological samples will be lawfully collected and processed. Medical research in human subjects will follow the procedures described in the **World Medical Association's Declaration of Helsinki**³ and the **Oviedo Bioethics Convention**⁴ (Convention on Human Rights and Biomedicine). In addition, all procedures will comply with **National law** and the **European Union's General Data Protection Regulation**⁵ (GDPR). Relative procedures will follow the **ICH Guidelines for Good Clinical Practice E6(R2)**⁶ and the **Good Clinical Practice Directive 2005/28/EC**⁷. **Collection, use, storage and otherwise processing of human genetic data, and of the biological samples from which they are derived will comply with UNESCO's Universal Declaration on the Human Genome and Human Rights**⁸ and **International Declaration on Human Genetic Data**⁹. Standards of quality and safety for the donation, procurement, testing, processing, preservation, storage and distribution of human tissues and cells according to the **Directive 2004/23/EC**¹⁰ is not applicable as human cells and tissues will not be used for patient treatment and transplantation.

More specifically, CARDIOCARE will comply with the principles of the **Charter of Fundamental Rights of the European Union**:

- Art. 1: respect of the dignity of human being as a whole;
- Art. 2: granting that the collected information will be used only in service of the human being and his right to life;
- Art. 3; II 1-III 2, 3c -dealing with medicine and biology, assure the application of the rule of informed consent to collect and store data; transparency on the scope and employment of the collected medical data (ref. also to art. 8); preventing and prohibiting the misuse of the stored information for eugenic purposes; preventing and prohibiting commerce of the human body for personal gain; preventing and prohibiting cloning;
- Art. 7: respect of the right to private life of the individual;
- Art. 21: preventing and avoiding any kind of discrimination on the ground of the collected information;
- Art. 23: gender equality;

¹ http://www.europarl.europa.eu/charter/pdf/text_en.pdf

² https://www.echr.coe.int/Documents/Convention_ENG.pdf

³ <https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/>

⁴ <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/164>

⁵ <https://gdpr-info.eu/>

⁶ http://www.ema.europa.eu/docs/en_GB/document_library/Scientific_guideline/2009/09/WC500002874.pdf

⁷ https://ec.europa.eu/health/sites/health/files/files/eudralex/vol-1/dir_2005_28/dir_2005_28_en.pdf

⁸ <http://www.unesco.org/new/en/social-and-human-sciences/themes/bioethics/human-genome-and-human-rights/>

⁹ <http://www.unesco.org/new/en/social-and-human-sciences/themes/bioethics/human-genetic-data/>

¹⁰ <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1399631190544&uri=CELEX:02004L0023-20090807>

- Art. 25: the right of the elderly, with a particular regard to special needs and care in term of medical and bioclinical care;
- Art. 26: the right of people with disability, with a particular regard to special needs and care in terms of medical and bio-clinical care;
- Art. 35: the right to access to a preventive healthcare system and to medical treatment to grant the protection of human health;
- (I 1, 4): clinical research to be performed on the moral principles for experimentation must be preceded by a careful assessment of risks;
- (II 2): combination of research with care to be performed accordingly to the therapeutic value for the involved subjects;
- (III 4a): researchers must act accordingly to safeguard the integrity of the individual, especially if the individual’s conditions and the information provided rely on the researcher’s performance.

Besides the international and EU ethical framework, relevant national legislation and guidelines are provided in Table 1. Data sharing between non-EU countries is not planned or anticipated.

Table 1: Relevant National legislation and guidelines.

Country	Relevant National legislation and guidelines
Greece (UOI, NKUA, FORTH, HMU)	<ul style="list-style-type: none"> ➤ Ministerial Decision 89292/2004 (which has implemented in Greece the Directive 2001/20/EC “on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use”. ➤ Ministerial Decisions G5a/59676/21.11.2016 (Government Gazette issue No. 4131/B/22.12.2016) in accordance with EU Regulation No. 536/2014 of the European Parliament and of the Council of 16 April 2014 on the clinical trials of medicinal products for human use. ➤ Act 2071/1992 (NHS) establishment of National Council of Medical Ethics and Deontology ➤ Data Protection Act 2472/1997 ➤ Regulation 4624/2019 - FEK 137/A/29-8-2019, incorporating GDPR into the National legislation ➤ Act 2667/1998 : National Bioethics Commission ➤ Act 2619/1998: ratification of the Oviedo Convention ➤ Ministerial Decision DYG3/89292/31.12.2003 (incorporating Directive 2001/20/EE into domestic law) ➤ Act 3418/2005 Code of Medical Ethics and Deontology
Italy (IEO, IMS)	<ul style="list-style-type: none"> ➤ Legislative Decree no.211 of June 24, 2003 “Transposition of Directive 2001/20/EC relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for clinical use”. ➤ C. M. n. 6 of 2 September 2002, Attività dei comitati etici istituiti ai sensi del decreto ministeriale 18 marzo 1998. (published on the G.U. n. 214 of 12 September 2002).



<p>Cyprus (BOCOC, STREMBLE)</p>	<ul style="list-style-type: none"> ➤ Law for Good Clinical Practice involving drugs for human use was introduced in 2001 and amended in 2004, implementing Directive 2001/20/EC. This law covers all interventional biomedical research projects. ➤ Law establishing the National Bioethics Committee was enacted in December 2001. This committee was initiated in 2002. ➤ Operational guidelines for the establishment of ethics committees (ECs) in reviewing biomedical research involving human subjects were published in 2004. ➤ Safeguarding and protection of the patients' rights law, Office of the Law Commissioner, Nicosia, 2005. ➤ The processing of personal data (protection of individuals), Republic of Cyprus, Law 2001. ➤ The Bioethics (Establishment and Function of the National Committee) Law of 2001.
<p>Netherlands (PHILIPS)</p>	<ul style="list-style-type: none"> ➤ Research involving human subjects has been legally regulated since 1999 via the Medical Research Involving Human Subjects Act (WMO). A revised version of the WMO, which gives effect to the Directive 2001/20/EC, came into operation on 1 March 2006. ➤ Decree of 23 June 2003 containing rules for compulsory insurance in medical research involving human subjects (Medical Research(Human Subjects) Compulsory Insurance Decree). In Dutch this is called “Besluit verplichte verzekering bij medisch-wetenschappelijk onderzoek met mensen”. ➤ Decree of 3 January 2006, amending the Central Review of Medical Research Involving Human Subjects Decree (enlargement of medical research that requires central review). In Dutch this is called “Besluit centrale beoordeling”.
<p>FRANCE (ESC)</p>	<ul style="list-style-type: none"> ➤ Loi n° 2004-806 du 9 août 2004 relative à la santé publique. Journal Officiel de la République Française. Articles 88-97, 11 août 2004 [online]. Available from URL: http://www.legifrance.gouv.fr/WAspad/VisuPcid=712996&indice=1&table=JORF&ligneDeb=1 ➤ Guide pratique sur l'encadrement de la recherche biomédicale. Les conditions de mise en œuvre de la recherche biomédicale. Code de la santé publique. Dispositions introduites par la loi n°2004–806 du 9 août 2004 relative à la politique de santé publique (JO du 11 août 2004). Article L1121–11. http://docplayer.fr/7150908-Guide-pratique-sur-l-encadrement-de-la-recherche-biomedicale-les-conditions-demise-en-oeuvre-de-la-recherche-biomedicale.html. ➤ LOI no. 2012-300 du 5 mars 2012 relative aux recherches impliquant la personne humaine. NOR: SASX0901817L. JORF n°0056 du 6 mars 2012. P: 4138. https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025441587&categorieLien=id. ➤ Loi n° 2004-806 du 9 août 2004 relative à la politique de santé publique. ➤ Loi n° 2004-800 du 6 août 2004 relative à la bioéthique.

	<ul style="list-style-type: none"> ➤ Rapport d'information fait au nom de la commission des Affaires sociales sur l'état d'application de la loi n° 2004-800 du 6 août 2004 relative à la bioéthique, par M. Alain MILON, sénateur (annexe au procès-verbal de la séance du 12 avril 2006). ➤ Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé.
Sweden (KSBC)	<ul style="list-style-type: none"> ➤ Research on humans is regulated by Law SFS 2003:460 and the updated Law SFS 2019:144 ➤ Since 2018 the Swedish Legislation complies with the EU General Data Protection Regulation, for the protection of personal data.
Slovenia (IOL)	<ul style="list-style-type: none"> ➤ Medicinal Products Act (Official Gazette of the Republic of Slovenia, No. 31/06 – ZZdr-1); Law on Medical Practice (Ur.l. RS, No.:98/99 and 67/02.), and Art. 47 on medical interventions informed consent procedures ➤ The Slovenian Code of Medical Deontology, Articles 47-50 with provisions on ethical conduct of biomedical research on human subjects. ➤ Act Amending the Medicinal Products and Medical Devices Act (Official Gazette of the Republic of Slovenia, No. 45/06 – ZZdr-1A ➤ Drug Act (Official gazette, No. 31/06) and Bylaw on Clinical Trials (Official gazette, No. 54/06), which is the Slovenian Directive on Clinical Drug Testing based on Directive 2001/20/EC.



4 Ethics and legal issues monitoring

For the monitoring of the ethical and legal aspects during the lifecycle of the CARDIOCARE project, Task 6.1 of WP6 has been provisioned, which is led by UOI. Key activities will be carried out during the project to ensure that all ethical standards and guidelines of Horizon 2020 will be rigorously applied and medical research will comply with international and EU conventions, declarations and regulations. In addition, a GDPR implementation plan has been devised to ensure a Data Protection by Design strategy from the beginning of the project. Furthermore, two dedicated boards have been formed to address all ethical and regulatory aspects of the project, the Ethical Advisory Board (EAB) and the Regulatory Advisory Board (RAB).

4.1 Ethical Advisory Board (EAB)

The ethical advisory board has been established to monitor and report on the legal, ethical, data protection, privacy, and security aspects of the project's activities during its lifecycle. EAB is formed by one member from IMS and ESC, the lead investigators from each clinical centre (IEO, BOCOC, KSBC, UOI, NKUA, IOL) and one member from ICOS and EUROPA DONNA. EAB will provide its reports as a deliverable submitted together with each periodic report of the project. Table 2 presents the members of the EAB, including two **external members** from ICOS and EUROPA DONNA.

Table 2: EAB members

No	Ethical Advisory Board members	Partner
1	Dr. Costanza Conti (cconti@ist-ims.it , Chair of EAB)	IMS
2	Prof. Gabriella Pravettoni (Gabriella.Pravettoni@ieo.it)	IEO
3	Dr. Anastasia Constantinidou (anastasia.constantinidou@bococ.org.cy)	BOCOC
4	Dr. Andri Papakonstantinou (andri.papakonstantinou@ki.se)	KSBC
5	Prof. Davide Mauri (dvd.mauri@gmail.com)	UOI
6	Dr. Nikolaos Memos (nikolaosmemos@gmail.com)	NKUA
7	Prof. Boštjan Šeruga (BSeruga@onko-i.si)	IOL
8	Christopher Plummer (chris.plummer@ncl.ac.uk , ESC Council of Cardio-Oncology)	ESC
9	Dr. Daniel Lenihan (djlenihan@wustl.edu , External member ICOS)	-
10	Dr. Antonella Moreo (antonella.moreo@gmail.com External member EUROPA DONNA)	-



4.2 Regulatory Advisory Board (RAB)

The role of the RAB is to monitor and report on the progress of Task 6.2 Analysis of regulatory aspects, with the aim to assess the regulatory roadmap towards the presentation of the new CARDIOCARE model and risk stratification concept in the regulatory experts during the final ESC workshop with EU policy makers, medical and patient associations. RAB is formed by the Project Coordinator (Prof. Fotiadis D., UOI), the Scientific Manager (Prof. Curigliano G., IEO), the Technical Manager (Prof. Marias K., FORTH), the Clinical Study Manager (Prof. Pravettoni G., IEO), an IMS member, head of the RAB (Dr. Costanza Conti), an ESC member (Riccardo Asteggiano) and an external member by EUROPA DONNA (Dr. Antonella Moreo) Table 3 presents the members of the RAB.

Table 3: RAB members

No	Regulatory Advisory Board members	Partner
1	Prof. Dimitrios Fotiadis (fotiadis@uoi.gr , Project Coordinator)	UOI
2	Prof. Giuseppe Curigliano (giuseppe.curigliano@ieo.it , Scientific Manager)	IEO
3	Prof. Kostas Marias (kmarias@ics.forth.gr , Technical Manager)	FORTH
4	Prof. Gabriella Pravettoni (Gabriella.Pravettoni@ieo.it , Clinical Study Manager)	IEO
5	Dr. Costanza Conti (cconti@ist-ims.it , Chair of RAB)	IMS
6	Dr. Riccardo Asteggiano (asteggianoricc@hotmail.com , ESC Council of Cardio-Oncology)	ESC
7	Dr. Antonella Moreo (antonella.moreo@gmail.com , External member EUROPA DONNA)	-



5 CARDIOCARE compliance with ethical standards and guidelines

Medical research will comply with international and EU regulations, conventions and declarations following guidelines for Good Clinical Practice. No human studies will commence before an ethics approval by the competent ethics committee has been obtained.

5.1 Informed Consent Procedures

For the informed consent procedures, when applicable, the following information and documents must be provided to the study participants.

- 1) Patient Information Sheets and Informed Consent Forms in native language and terms understandable to the participants.
- 2) The rights of the participants including the right:
 - To know that participation is voluntary.
 - To ask questions and receive understandable answers before making a decision.
 - To know the degree of risk and burden involved in participation.
 - To know who will benefit from participation.
 - To know the procedures that will be implemented in the case of **incidental findings**.
 - To receive assurances that appropriate insurance cover is in place.
 - To know how their biological samples and data will be collected, protected during the project and either destroyed or reused at the end of the research.
 - To withdraw themselves, their samples and data from the project at any time
 - To be informed that in case of withdrawal from the study this will not affect their treatment options or their relationship with their physician
 - To know of any potential commercial exploitation of the research.

In addition, according to **Article 13 of the General Data Protection Regulation (GDPR)** the following information must be provided where personal data are collected from the patients:

- 3) The identity and the contact details of the controller.
- 4) The contact details of the data protection officer (DPO), where applicable.
- 5) The purposes and legal basis for the processing for which the personal data are intended.
- 6) The recipients or categories of recipients of the personal data.
- 7) The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.
- 8) The existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability.
- 9) Where the processing is based on consent the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.
- 10) The right to lodge a complaint with a supervisory authority.
- 11) The existence of **automated decision-making including profiling**, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.



5.1.1 Language and terms

Information sheet and consent form should be translated from English to each native language. Information presented in these documents shall be provided in an intelligible and easily accessible manner, using clear and plain language. Any technical or scientific wording must be clearly explained or replaced with simplified terminology. Patients will be informed that before making any decision they should ask any questions they have and receive understandable answers. Information sheet and informed consent form should have appropriate pagination illustrating the consecutive page numbering and total number of pages.

5.1.2 Copies of the Informed Consent Forms, Information Sheets & Ethical Approvals

No human studies will commence before an ethics approval by the competent ethics committee has been obtained. Informed consent documents will be signed in two copies, one copy for the patient and one copy for the study team. Document templates and copies of the patients' signed Informed Consent Forms will be kept on file, by the principal investigator of each clinical centre, and submitted upon request to the European Commission. Copies of ethical approvals by each competent local Ethics Committee must be kept on file and submitted upon request to the European Commission.

5.1.3 Incidental Findings Policy

The study involves clinical, genomic, biochemical and imaging (Echocardiography) procedures as well as sensor monitoring of health status that may lead to incidental findings regarding patient's health, not related to the purposes of the study. The project's policy is to disclose such incidental findings to the patient him/herself only, unless he, or she, prefers not to. Disclosure of incidental findings must rely on evidence-based best practices. Patient's preferences about disclosing of such findings should be and will be taken into account in a specific question at the Informed Consent Form

5.1.4 Patient 'Profiling' involving tracking or observation of participants

CARDIOCARE research involves 'profiling' of patients enrolled in the prospective clinical study which is an observational, parallel cohort study with control and supportive care arms. The specific 'profiling' involves automated processing of personal data about the intrinsic capacity of the patient, collected by wearable sensor and mobile health application data sources in order to monitor aspects of patients' health, behaviour, location and movements. **However, such 'profiling' DOES NOT involve automated individual decision-making, with legal or similarly significant effects for the participants.** Automated processing using machine learning techniques will be applied for the development of the CARDIOCARE risk stratification model. Patients will be informed of the existence of the profiling, any possible consequences and their rights in the Informed Consent Form for their participation in the prospective clinical study as well as in a Privacy Notice providing data subjects with GDPR Article 13 information enabling them to exercise their rights at any time. In addition, a **Data Protection Impact Assessment (DPIA)** will be carried out by each clinical centre (Data Providers) in order to assess any risks arising from the processing activities planned, including profiling, and to assess the effectiveness of the technical and organisational measures taken for the protection of the rights and freedoms of the data subjects.



5.2 Human cells / tissues obtained within the project

Whole blood and stool sampling will be performed for the purposes of the prospective clinical study. Blood samples will be collected before, during and at follow up time points after chemotherapy. Whole blood and plasma will be used for routine lab tests, biochemical biomarkers (Troponin I, NT-pro BNP), inflammatory/psychomarkers (platelet activation, IL-6, TNF- α , HRV, CRP, Fibrinogen, Ferritin) and -omics biomarkers (SNPs, liquid biopsies, extracellular vesicles miRNAs). Specifically, analyses of Single Nucleotide Polymorphisms (SNPs) will be performed by DNA extraction of collected. Peripheral Blood Mononuclear Cells (PBMCs), comprising peripheral blood cells having a round nucleus. These cells consist of lymphocytes (T cells, B cells, NK cells) and monocytes, whereas erythrocytes and platelets have no nuclei, and granulocytes (neutrophils, basophils, and eosinophils) have multi-lobed nuclei. In humans, lymphocytes make up the majority of the PBMC population, followed by monocytes, and only a small percentage of dendritic cells. These cells can be extracted from whole blood using ficoll, a hydrophilic polysaccharide that separates layers of blood, and gradient centrifugation, which will separate the blood into a top layer of plasma, followed by a layer of PBMCs and a bottom fraction of polymorphonuclear cells (such as neutrophils and eosinophils) and erythrocytes. Stool samples will be collected (n=500) in a subpopulation of patients (IEO: 100, BOCOC: 100, KSBC: 80, NKUA: 130, IOL: 90) before, and 3 months after treatment. Metagenomic analysis of stool samples will be performed for microbiome biomarkers.

5.3 GDPR implementation plan

The GDPR implementation plan provides guidance on how the data processing activities shall be performed in a **lawful, fair and transparent manner** implementing principles of **data minimisation** and **purpose limitation**. Data integrity and confidentiality shall be ensured by using appropriate technical and organisational measures based on a **Data Protection by Design strategy** to safeguard the rights and freedoms of the data subjects. To this end, appropriate **Data Sharing Agreements** for Joint Controllers shall be signed by the consortium and any involved third parties. In addition, Data providers shall perform comprehensive **Data Protection Impact Assessments (DPIAs)** in order to assess any potential risks arising from the processing activities planned and to assess the effectiveness of the technical and organisational measures taken for the protection of the rights and freedoms of the data subjects. No processing activities will proceed before obtaining an approval by the **Data Protective Officers (DPOs)** of the respective organisations and institutions. Complementary to the previous measures, a **Privacy Notice** shall also be devised in plain language, providing data subjects with GDPR Article 13-14 information enabling them to exercise their rights at any time. All data transfers shall be performed via the developed Data management platform (WP5) implementing appropriate organisational and **security measures**.

The following information and guidelines are provided for the consistent implementation of the Regulation by all partners of the CARDIOCARE project.

5.3.1 GDPR Scope

The General Data Protection Regulation (GDPR) is the new EU's regulation repealing the previous Data Protection Directive and it is designed to protect and empower every subject's data privacy located in the EU regardless of where the processing is taking place. Furthermore, the GDPR applies to every organisation located in the EU that processes personal data regardless of the data subject's nationality and covers several activities and aspects including data collection, processing, transfer, storage, security, and the data subject rights.

GDPR has been enforced on May 25th 2018 and non-compliance can be fined up to 4% of annual global turnover or €20 Million. Fines will be served by the national Data Protection Authorities (DPAs).

GDPR affects members of the European Economic Area¹¹ (EEA), including Iceland, Liechtenstein, Norway and the United Kingdom (UK). In simple words personal data which are processed inside the EEA (blue area in figure 2), imported in or exported out of the EEA for processing are protected by GDPR.

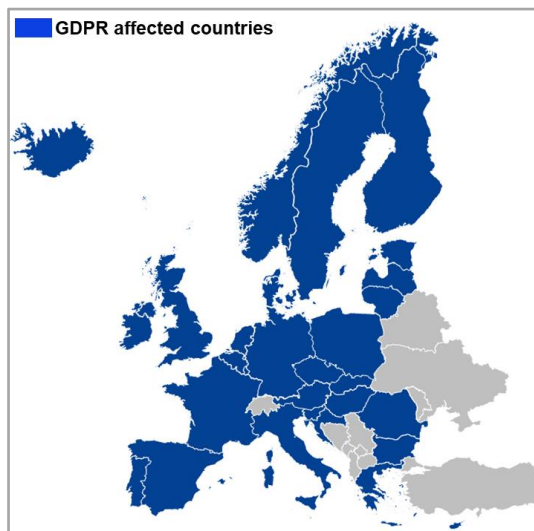


Figure 2: GDPR is applied in both EU and EEA countries.

GDPR comprises 11 chapters which include 99 Articles with one or more sub-articles for the protection of personal data. The 99 Articles were adopted considering 173 Recitals. Although Articles and Recitals are complementary to each other, the Court of Justice of the European Union uses Recitals to establish any Regulation's or Directive's meaning. Guidelines for the consistent implementation of the GDPR are provided by Article 29 Working Party (WP29)¹² comprising members of each Member State Data Protection Authority (DPA). The WP29 has been renamed to European Data Protection Board (EDPB) with enhanced roles on providing guidelines and decisions.

5.3.2 GDPR definitions

The following definitions are necessary for the communication of the GDPR.

Personal data: any information relating to an identifiable natural person e.g. name, ID, location, online identifier, physical, health (Recital 35), genetic (Recital 34), biometric, mental, economic, cultural or social data.

Genetic data: personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in

¹¹ <http://www.efta.int/EEA/news/Incorporation-GDPR-EEA-Agreement-508041>

¹² http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358



question, in particular chromosomal, DNA or RNA analysis, or from the analysis of another element enabling equivalent information to be obtained.

Health data: personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status. Information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

Processing: any operation performed on personal data whether or not by automated means e.g. collection, recording, organization, structuring, storage, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, combination, restriction, erasure or destruction.

Pseudonymisation: the processing of personal data in such a manner that the personal data can no longer be attributed to a person without the use of additional information kept separately and secured by means of technical and organisational measures. **Pseudonymized data are still personal data subject to GDPR.**

Anonymous data: information which does not relate to an identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. GDPR **does not concern** the processing of such **anonymous information**, including for statistical or research purposes (Recital 26).

Controller and joint Controller: the person, authority, or other body which, alone or jointly, determines the purposes and means (the why and how) of the processing of personal data.

Processor: a person, authority, or other body which processes personal data on behalf of the controller.

Data Protection Officer (DPO): a staff member or a professional on the basis of a service contract who has expert knowledge of data protection law and practices

- Is able to monitor compliance with GDPR and provide advice
- Communicates with the supervising authority (DPA)
- Is accessible to data subjects with regard to the exercise of their rights.

5.3.3 GDPR Principles

GDPR applies seven principles that all CARDIOCARE partners engaged with processing activities, must comply with.

- **Lawful, fair and transparent processing** (legal basis e.g. on consent, otherwise purpose compatibility or scientific purpose exemption under appropriate safeguards such as encryption or pseudonymization)
- **Purpose limitation** (data not further processed in a manner that is incompatible with the initial purposes)
- **Data minimisation** (limited to what is necessary in relation to initial purposes)



- **Accuracy** (data updated and rectified where necessary)
- **Storage limitation** (data kept in a form which permits identification of data subjects for no longer than is necessary for the purposes of the study (exceptions: scientific research purposes with the appropriate safeguards including technical and organisational measures required)
- **Integrity and confidentiality** (protection against unlawful processing, accidental loss, destruction or damage)
- **Accountability** (controller and processor shall be able to demonstrate compliance with previous points)

5.3.4 Data Protection by Design strategy

CARDIOCARE has implemented the following Data Protection by Design strategy, summarized in the following points:

- 1. Clear assignment of roles (who is a joint controller and who is a processor).**
 - **Joint Controllers:** All CARDIOCARE partners engaged in processing activities of patient data will be **Joint Controllers**, including the **Data Providers** who shall collect and share retrospective and/or prospective data with the **Data Recipients** who will perform further processing activities.
 - **Processors:** Any third parties who will process patient data on behalf of the joint controller and under their specific instructions under a contract.
- 2. Specific Data Sharing Agreement and contracts made between joint controllers and processors.** Data Sharing Agreements between joint controllers, and Contracts in case of any processors, must contain information described in Articles 26 and 28, respectively. The **CARDIOCARE Data Sharing Agreement for Joint Controllers** is provided in the **Appendix**.
- 3. Specific legal basis for processing** that can be demonstrated by all partners.
 - **For the purposes of further processing retrospective data, lawful processing is based on the following legal grounds:**
 - a. Processing is necessary for the performance of a task carried out in the public interest according to Article 6(1e) of the GDPR. The task or function has a clear basis in law in line with Recital 45 of the GDPR. In case of not a public body processing is necessary for the legitimate interests pursued by the beneficiary according to Article 6(1f).
 - b. Further processing is based on scientific research purposes as a lawful compatible purpose, in line with Recitals 50 and 159 of the GDPR.
 - c. Additional condition for processing sensitive / special category data including health data is that processing is necessary for scientific research purposes in the public interest and in the area of public health according to Article 9(2j) and Recitals 52, 53 and 159 with appropriate safeguards in line with Article 89(1) and Recitals 156 and 157 of the GDPR.



➤ **For the purposes of processing newly collected data from patients enrolled to the CARDIOCARE prospective clinical study, lawful processing is based on the following legal grounds:**

- a. Processing is necessary for the performance of a task carried out in the public interest according to Article 6(1e) of the GDPR. The task or function has a clear basis in law in line with Recital 45 of the GDPR. For non-public bodies, processing is necessary for the legitimate interests in scientific research pursued by the beneficiaries according to Article 6(1f) of the GDPR.
- b. Additional condition for processing sensitive / special category data including health data is that processing is necessary for scientific research purposes in the public interest and in the area of public health according to Article 9(2j) and Recitals 52, 53 and 159 with appropriate safeguards in line with Article 89(1) and Recitals 156 and 157 of the GDPR.

4. Make a Privacy Notice publicly available providing, where applicable, Article 13 & 14 information to the data subject enabling them to exercise their rights. Data Providers undertake to inform the data subjects, via their institution's website, with the information listed in Articles 13 and 14 of the GDPR, including their rights and how to exercise them to comply with the principle of transparency.

➤ **Based on the legal grounds used for further processing retrospective data, the Data Subjects are entitled to the following rights:**

- a. The right to be informed, the right of access and the right to rectification.
- b. Based on the specific legal grounds for processing, the rights to erasure, to data portability, and to object are NOT available in line with Recital 65 and Article 17(3d), Recital 68, and Article 21(6) plus Recital 159 of the GDPR respectively.

➤ **Based on the legal grounds used for processing newly collected data from patients enrolled to the prospective clinical study, the Data Subjects are entitled to the following rights:**

- a. Processing The right to be informed, the right of access and the right to rectification.
- b. Based on the specific legal grounds for processing, the rights to erasure, to data portability, and to object are NOT available in line with Recital 65 and Article 17(3d), Recital 68, and Article 21(6) plus Recital 159 of the GDPR respectively.

As an example the **UOI Privacy Notice** is provided in the **Appendix**.

5. Implementation of appropriate safeguards. Each joint controller acting as a Data Provider has full control of its data which must **pseudonymise** holding the key code in separate location, and before the data is transferred for further processing. Pseudonymized data are still personal data subjected to the GDPR. Importantly, if data are appropriately anonymized GDPR does not apply and such data can be freely transferred and processed.



6. **Keep records of all processing activities:** Each joint controller is responsible to maintain a record of all of its processing activities in electronic form with specific information described in Article 30 and provided to supervisor authority or data subject upon request.
7. **Designation of a Data Protection Officer (DPO):** Each joint controller acting as a Data Provider, where patient (health and genetic) data are processed (including collection) should take appropriate measures to designate a DPO as described in Articles 37, 38, 39.
8. **Perform a Data Protection Impact Assessment (DPIA):** Joint Controllers acting as Data Providers, taking their DPO's opinion and advice shall carry out an impact assessment of the risks that may be arise by the overall processing activities planned, as described in Article 35. **No processing activities shall proceed without the written advice/opinion of the DPO.** The templates provided by the Information Commissioner's Office (ICO), UK's Data Protection Authority¹³ were selected to perform the DPIAs in the project. If a joint controller's (acting as a Data Provider) impact assessment indicates a high risk for data protection, controller shall consult (prior consultation) the supervisor authority (DPA), as described in Article 36. As an example, the **UOI DPIA** with the **DPO approval** is provided in the **Appendix**.
9. **Data transfers and security:** Data transfers between Joint Controllers shall be performed using the Cloud infrastructure provided by FORTH (an EU-based partner) acting as a Data Recipient and Joint Controller. Considering the risks arising from the processing activities involved, the Joint Controllers shall implement strategies of data protection with a level of security appropriate to those risks, including but not limited to:
 - a. **Pseudonymisation** of the personal data or biological samples by the Data Providers, before uploading the data to the cloud for transferring and/or further processing. The key codes shall be kept in separate location from the Personal Data.
 - b. **Encryption** of the Personal Data stored within the cloud, to prevent unauthorised and unlawful processing, including Password Storage Encryption, Data Partition Encryption and SSL Host Authentication. Secure and separate access to each joint controller shall be provided only upon entering into this Agreement.
 - c. Appropriate **back-up procedures** to avoid accidental loss, destruction or damage of the Personal Data by a physical or technical incident, enabling to reinstate the system in a timely manner.
 - d. **Secure biological sample storage conditions** including equipment maintenance and authorised processing of the samples by trained personnel only, to avoid accidental loss, destruction or damage of the biological samples by a physical or technical incident.
 - e. **Audit Log operation** to allow viewing the users' access history to the system enabling the detection of any potential security or data breaches.
 - f. Conducting **regular security assessments** on systems to review the effectiveness of the security measures and on biological sample storage conditions.

¹³ <https://ico.org.uk/media/for-organisations/documents/2258857/dpia-template-v1.docx>

- g. Ensuring that pseudonymised personal data will **not be stored outside the European Economic Area (EEA)**.
- h. Ensuring all research personnel have been made aware of their responsibilities concerning the handling of Personal Data and commit to a duty of confidence by signing a **non-disclosure declaration**.

Collectively, the role of each CARDIOCARE partner as a joint controller (Data Provider or Data Recipient), the categories of data provided including retrospective and prospective data, the data processing activities, cloud data transfers and Data Sharing Agreements are illustrated in **Figure 3**.

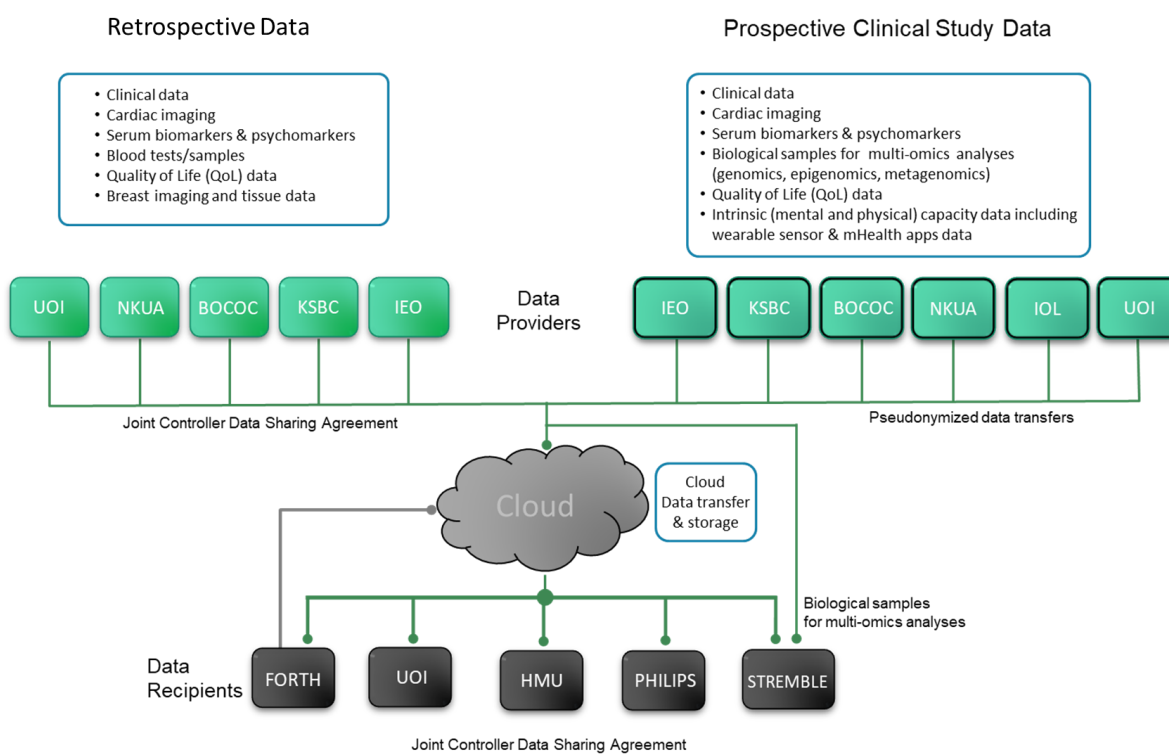


Figure 3: Data categories, Roles, Data Sharing Agreement, and data transfers.

D6.1. – Implementation of ethical standards and guidelines of H2020 and GDPR implementation plan



6 Conclusions

Deliverable 6.1 presents the ethical standards and guidelines of Horizon 2020 that must be applied by all CARDIOCARE partners. To follow a Data Protection by Design strategy a GDPR implementation plan has been devised providing guidance on how the data processing activities shall be performed in a lawful, fair and transparent manner. **Significant updates** and any complementary information on all legal, ethical, data protection, privacy and security aspects during the project's lifecycle **will be reported by the EAB as a deliverable submitted together with each periodic report of the project.**

D6.1. – Implementation of ethical standards and guidelines of H2020 and GDPR implementation plan



7 Appendix (Data Sharing Agreement, Privacy Notice & DPIA-UOI)

Data Sharing Agreement



Version 2.0 as of December 2021

in supplementation to the rules set by the EC Grant Agreement No. 945175 of the Horizon 2020 project entitled:

**“AN INTERDISCIPLINARY APPROACH FOR THE
MANAGEMENT OF THE ELDERLY MULTIMORBID
PATIENT WITH BREAST CANCER THERAPY INDUCED
CARDIAC TOXICITY - CARDIOCARE”**

(“the Project”)

made on 17 December 2021 (“Effective Date”)

PARTIES

PANEPISTIMIO IOANNINON (**UOI**), established in PANEPISTEMIOYPOLE
PANEPISTEMIO IOANNINON, IOANNINA 45110, Greece, VAT
number: EL090029284;

ISTITUTO EUROPEO DI ONCOLOGIA SRL (**IEO**), established in Via
Filodrammatici 10, MILANO 20121, Italy, VAT number:
IT08691440153;

OGKOLOGIKO KENTRO TRAPEZAS KYPROU (**BOCOC**), established in
LEOFOROS AKROPOLEOS 32, STROVOLOS 2006, Cyprus, VAT
number: CY90004583G;

IDRYMA TECHNOLOGIAS KAI EREVNAS (**FORTH**), established in N
PLASTIRA STR 100, IRAKLEIO 70013, Greece, VAT number:
EL090101655;

PHILIPS ELECTRONICS NEDERLAND BV (**PHILIPS**), established in HIGH
TECH CAMPUS 52, EINDHOVEN 5656 AG, Netherlands, VAT
number: NL001902106B01;

REGION STOCKHOLM (**KSBC**), established in HANTVERKARGATAN 45,
STOCKHOLM 104 22, Sweden, VAT number: SE232100001601;

STREMBLE VENTURES LTD (**STREMBLE**), established in KO 8
GERMASOGEIA, LIMASSOL 4045, Cyprus, VAT number:
CY10300648F;

ONKOLOSKI INSTITUT LJUBLJANA (**IOL**), established in ZALOSKA CESTA
2, LJUBLJANA 1000, Slovenia, VAT number: SI34052674;

ETHNIKO KAI KAPODISTRIAKO PANEPISTIMIO ATHINON (**NKUA**),
established in 6 CHRISTOU LADA STR, ATHINA 10561, Greece, VAT
number: EL090145420;

ELLINIKO MESOGEIAKO PANEPISTIMIO (**HMU**), established in
ESTAVROMENOS, HERAKLION 71004, Greece, VAT number:
EL996844271,

Individually referred to as a “**Party**” or collectively referred to as the “**Parties**”

BACKGROUND

The **Parties** are acting as **Joint Controllers** on behalf of the **CARDIOCARE project**, which has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 945175, entitled: "AN INTERDISCIPLINARY APPROACH FOR THE MANAGEMENT OF THE ELDERLY MULTIMORBID PATIENT WITH BREAST CANCER THERAPY INDUCED CARDIAC TOXICITY".

The **Parties** agree to share the Personal Data on terms set out in this Agreement which explains the purposes for which that Personal Data may be used.

AGREED TERMS

1. INTERPRETATION

The following definitions and rules of interpretation apply in this agreement.

Definitions:

Privacy and Data Protection Legislation: The EU Regulation 'GDPR' 2016/679 and all applicable national and international laws and regulations relating to the processing of the personal data and privacy, and the equivalent of any of the foregoing in any relevant jurisdiction, (e.g. in the UK, the national data Protection Legislation, the Human Rights Act 1998, the European Convention on Human Rights, the General Data Protection Regulation (References to legislation include any amendments made to those laws from time to time.

The Project: The CARDIOCARE project.

Agreed Purposes: has the meaning given to it in Clause 3 of this Agreement.

The Agreement: this Agreement.

Business Day: a day other than a Saturday, Sunday or public holiday in the countries of each Party when banks are open for business.

The Tasks: the tasks the Parties are contracted to carry out under the EC Grant Agreement No. 945175 in order to provide the relevant deliverables.

Joint Controllers: According to Article 26(1) GDPR where two or more controllers jointly determine the purposes and means of processing of personal data, they shall be joint controllers.

Data Provider(s): means one (or more) of the Parties, acting as joint controller(s), whose role in the Project involves the provision of personal data to the Project, including data transferring to the Data Recipients, for the purposes and tasks set out in the Annex 1

(‘Description of the action’) of the EC Grant Agreement No 945175 and specified in Schedule 1 to this Agreement.

Data Recipient(s): means one (or more) of the Parties, acting as joint controller(s), whose role in the Project involves the use and analysis of personal data provided to the Project by the Data Providers, for the purposes and tasks set out in the Annex 1 (‘Description of the action’) of the EC Grant Agreement No 945175 and specified in Schedule 1 to this Agreement.

Data Processor: means a natural or legal person, public authority, agency or other body which processes personal data on behalf of a controller.

Lead Data Protection Authority: the supervisor authority of each Data Provider.

The Data Protection Authorities Concerned: the supervisor authorities of the Data Recipients.

The Personal Data: means personal data as defined in the GDPR, any information relating to an identified or identifiable natural person, including health and genetic data detailed in Schedule 2 and to be shared between the parties under Clause 4 of this Agreement.

Subject Access Request: means the "Right of access by the data subject" in Article 15 of the GDPR.

Term: shall mean the **duration** of the data sharing agreement which shall remain in force for the duration of the Project, but until **June 30th 2025**, unless an extension of the Project duration is granted by the European Commission.

Data Subject, sensitive/special category data, pseudonymisation, personal data breach, processing, third party, supervisory authority and appropriate technical and organisational measures shall have the meanings given to them in the GDPR.

Clause, Schedule and paragraph headings shall not affect the interpretation of this Agreement.

The Schedules form part of this Agreement and shall have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Schedules.

Unless the context otherwise, requires, words in the singular shall include the plural and, in the plural, shall include the singular.

References to Clauses and Schedules are to the Clauses and Schedules of this Agreement and references to paragraphs are to paragraphs of the relevant Schedule.

Any words following the terms including, include, in particular or for example or any similar phrase shall be construed as illustrative and shall not limit the generality of the related general words.

A reference to **writing** or **written** includes letter and email.

2. COMPLIANCE WITH DATA PROTECTION LAWS

2.1 The Parties acknowledge that under the GDPR, the Parties are acting as **Joint Controllers** where processing Personal Data under the terms of this Agreement.

2.2 Each Party must ensure compliance with the Privacy and Data Protection Legislation at all times during the Term of the Agreement.

3. AGREED PURPOSES

3.1 This **Agreement** sets out the framework for the sharing of Personal Data between the Parties. It sets out the **purposes** for which the Personal data may be processed by the Parties, the principles and procedures that the Parties shall adhere to, and the respective **responsibilities** of the Parties, in a transparent manner.

3.2 In order to carry out the Tasks set under the EC Grant Agreement No 945175 the Parties have to transfer Personal Data between the Parties. **Schedule 1** to this Agreement provides an outline of the Purposes for which the data sharing is necessary.

3.3 The Parties agree to only process the Personal data in accordance with the **instructions** set out in this Agreement, and only for the purposes described in **Schedule 1**. The Parties shall not process Personal Data in a way that is incompatible with the purposes described in this Clause (the Agreed Purposes).

3.4 Each party shall appoint a **Single Point of Contact (SPoC)** who will work together to reach an agreement with regards to any issues arising from the data sharing and to actively improve the effectiveness of the data sharing agreement. The points of contact for each of the parties are:

UOI SPoC – Professor Dimitris Fotiadis, Head of the Unit of Medical Technology and Intelligent Information Systems, Email: dimitris.fotiadis30@gmail.com, Tel:+302651009006.

IEO SPoC – Professor Gabriella Pravettoni, Applied Research Division for Cognitive and Psychological Science, Email: gabriella.pravettoni@ieo.it. Tel.:+390294372099.

BOCOC SPoC – Dr. Anastasia Constantinidou, Department of Medical Oncology, Email: Anastasia.constantinidou@bococ.org.cy, Tel.:+357 22847411.

FORTH SPoC – Associate Professor Kostas Marias, Computational BioMedicine Laboratory (CBML), Institute of Computer Science (ICS), Email: kmarias@ics.forth.gr, Tel.:+30 2810 391672.

PHILIPS SPoC – Dr. Anca Bucur, Precision and Decentralized Diagnostics Group, Email: anca.bucur@philips.com, Tel.:+31(0) 627229089

KSBC SPoC – Dr. Andri Papakonstantinou, Breast Centre, Karolinska University Hospital, Email: andri.papakonstantinou@ki.se, Tel.:0046 762732847.

STREMBLE SPoC – Dr. Athos Antoniadis, Chief Executive Officer, Email: athos.antoniadis@stremble.com, Tel.: +357 25004457.

IOL SPoC – Dr. Ribnikar Domen, Department of Medical Oncology, Email: dribnikar@onko-i.si, Tel.:00386 (0)40 163 480.

NKUA SPoC – Professor Manousos Konstadoulakis, 2nd Department of Surgery, Aretaieio University Hospital, Email: mkonstad@med.uoa.gr, Tel.:+302107286128.

HMU SPoC – Professor Manolis Tsiknakis, Department of Electrical and Computer Engineering, Email: tsiknaki@hmu.gr, Tel.:+302810 379885.

4. PERSONAL DATA

4.1 The Personal Data shared under this Agreement will comprise of Personal and **special category data** including clinical, imaging, biomarker, intrinsic capacity and QoL data, as well as wearable sensor and mobile Health application data collected by elderly breast cancer patients. A more detailed description of the categories of Personal Data processed under this Agreement is set out in **Schedule 2** to the Agreement.

4.2 The Parties agree that the Personal Data shared under this Agreement must be **pseudonymized** by the **Data Provider** before transferring to **Data Recipients** and not be irrelevant or excessive with regard to the Agreed Purposes set out in **Clause 3**, in order to **minimise** the amount of Personal Data shared.

4.3 The **Data Recipients** agree to process the Personal Data described in **Schedule 2**, only for the purposes outlined in **Clause 3** of this Agreement and strictly for no other purpose without the written authority of the **Data Provider**.

4.4 The **Data Recipients** will **NOT** disclose or share the Personal Data processed under the Agreement, with any third party without the written authority of the **Data Provider**.

4.5 The **Data Recipients** are prohibited from publishing any information related or produced by the Personal Data shared, including any results, without prior authorisation by the **Data Provider**.

5. FAIR, TRANSPARENT AND LAWFUL PROCESSING

5.1 Each Party shall ensure that it processes the Personal Data **in a fair, transparent and lawful manner** in accordance with the Privacy and Data Protection Legislation during the Term of this Agreement.

5.2 For the purposes of **further processing** patients' data available from other projects, as described in **Schedule 1, point I** to this Agreement, each Party will process shared Personal Data on the basis of the following **legal grounds**:

- a. Processing is necessary for the **performance of a task carried out in the public interest** according to Article 6(1e) of the GDPR. The task or function has a clear basis in law in line with Recital 45 of the GDPR. In case of non-public bodies, processing is necessary for the **legitimate interests in scientific research** pursued by the beneficiaries according to Article 6(1f) of the GDPR.
- b. Further processing is based on **scientific research purposes** as a lawful compatible purpose, in line with Recitals 50 and 159 of the GDPR.
- c. Additional condition for processing sensitive / special category data including health data is that processing is necessary for **scientific research purposes in the public interest and in the area of public health** according to Article 9(2j) and Recitals 52, 53 and 159 with appropriate safeguards in line with Article 89(1) and Recitals 156 and 157 of the GDPR.

5.3 For the purposes of processing newly collected data from patients enrolled to the CARDIOCARE prospective clinical study, as described in **Schedule 1, point II** to this Agreement, each Party will process shared Personal Data on the basis of the following **legal grounds**:

- a. Processing is necessary for the **performance of a task carried out in the public interest** according to Article 6(1e) of the GDPR. The task or function has a clear basis in law in line with Recital 45 of the GDPR. In case of non-public bodies, processing is necessary for the **legitimate interests in**

scientific research pursued by the beneficiaries according to Article 6(1f) of the GDPR.

- b. Additional condition for processing sensitive / special category data including health data is that processing is necessary for **scientific research purposes in the public interest and in the area of public health** according to Article 9(2j) and Recitals 52, 53 and 159 with appropriate safeguards in line with Article 89(1) and Recitals 156 and 157 of the GDPR.

5.4 For the purposes described in **Clause 5.2** and **5.3** of this Agreement the **Data Provider** undertakes to inform, where applicable, the data subjects with the information listed in **Articles 13** and **14** of the GDPR in order to comply with the principle of **transparency**.

6. DATA ACCURACY

6.1 The Parties agree to ensure that the Personal Data processed is **accurate** and kept **up to date**. The Parties agree to review the accuracy of the personal data and make any necessary changes to any Personal Data which is inaccurate or requires updating.

6.2 Where either Party becomes aware of inaccuracies in shared Personal Data, they will notify the other Parties.

7. DATA SUBJECTS' RIGHTS

7.1 For the purposes of processing patient data available from other projects based on the legal grounds of **Clause 5.2** of this Agreement, the Data Subjects are entitled to **the following rights**:

- a. The right to be informed, the right of access and the right to rectification.
- b. Based on the specific legal grounds for processing, the rights to erasure, to data portability, and to object are **NOT** available in line with Recital 65 and Article 17(3d), Recital 68, and Article 21(6) plus Recital 159 of the GDPR respectively.

7.2 For the purposes of processing newly collected data from patients enrolled to the CARDIOCARE prospective clinical study based on the legal grounds of **Clause 5.3** of this Agreement, the Data Subjects are entitled to **the following rights**:

- a. The right to be informed, the right of access and the right to rectification.
- b. Based on the specific legal grounds for processing, the rights to erasure, to data portability, and to object are **NOT** available in

line with Recital 65 and Article 17(3d), Recital 68, and Article 21(6) plus Recital 159 of the GDPR respectively.

- c. Any change in the lawful basis for processing must be notified to a Data Subject in accordance with the information requirements in Articles 13 and 14 of the GDPR and under the general principle of **transparency**.

7.3 Data Subjects can exercise their rights through a **Subject Access Request** to the respective **Data Provider**. If required, the **Data Recipients** agree to provide **full co-operation and assistance** to the Data Provider to enable him to comply with Subject Access Requests and to respond to any other queries or complaints. The Data Recipients agree to provide such assistance promptly and **no later than 5 Business Days** upon receipt by the Data Provider of a Data Subject request.

7.4 In case of any Subject Access Requests, queries or complaints received by the **Data Recipients**, the Data Recipients shall notify the Data Providers immediately [and no later than 48 hours] upon receipt in order to enable the Data Providers to respond promptly to the Data Subjects.

7.5 The Data Recipients agree to act only under the Data Provider's instructions in relation to any activities undertaken to resolve any complaints or comply with any requests from the Data Subjects under Clause 7.

7.6 To facilitate the Data Subjects' rights, the Parties agree to maintain **Records** of all Personal Data processed and **all processing activities** under the Agreement in a structured, commonly used and machine-readable form. In addition to the above Records, the Parties shall maintain a record of **Subject Access Requests** or **complaints** including the decisions made or measures taken and any information that was exchanged. The Data Providers reserve the right to **inspect** the records maintained by the Data Recipients under this Clause at any time.

8. DATA TRANSFERS

8.1 For the scientific research purposes of the Project the Parties shall share **pseudonymised** Personal Data using the **Private Cloud infrastructure** provided by FORTH (an EU-based Joint Controller) as specified in **Schedule 1** of the Agreed Purposes.

8.2 For the purposes of providing the Cloud Services (described in **Schedule 1**), the Cloud provider (FORTH) shall ensure that

pseudonymised Personal Data will not be stored outside the European Economic Area (EEA).

8.3 The Data Recipients agree NOT to engage any third parties without the prior **specific** written authorisation by the Data Providers.

8.4 In accordance with the Agreed Purposes, the Parties confirm that Data Transfers outside the EEA is NOT intended.

9. SECURITY

9.1 The Parties shall implement appropriate technical and organisational measures to protect the Personal Data shared, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed in accordance with Article 32 of the GDPR.

9.2 Specifically, taking into account the Agreed Purposes (Clause 3), the nature of the Personal Data shared (Clause 4), the state of the art, the costs of implementation, as well as the risks arising from such processing activities for the rights and freedoms of the Data subjects, the Parties shall implement appropriate technical and organisational measures to ensure a level of security appropriate to those risks, including but not limited to the measures specified in **Schedule 3** to this Agreement. The Parties agree to assist each other in meeting their obligation to keep the Personal Data shared secure and notify each other of any changes to the measures described in **Schedule 3**.

9.3 The Data Recipients agree to allow for inspections and assessments to be undertaken by the Data Providers in respect of the security measures taken, or to provide evidence of those measures if requested.

10. DATA PROTECTION IMPACT ASSESSMENT (DPIA)

10.1 The Data Recipients as Joint Controllers with the Data Providers shall provide assistance to each Data Provider in meeting Article 35 obligation of the GDPR to carry out a Data Protection Impact Assessment, in relation to Processing of the Personal Data shared and taking into account any future changes on the risks represented by processing operations that might require a review of the original Data Protection Impact Assessment.

10.2 Where a DPIA referred to Clause 10.1 indicates an **unmitigated high risk** to the processing operations, the Data Recipients shall assist the

Data Provider in meeting the **Prior Consultation** obligation with its Supervisory Authority in accordance of Article 36 of the GDPR.

11. PERSONAL DATA BREACHES AND REPORTING PROCEDURES

- 11.1 The Data Recipients are under a strict obligation to immediately notify the Data Providers of any **Personal Data Breach** and no later than **24 hours** upon the Data Recipients' becoming aware of the breach. The Data Recipients shall provide all available information for the breach in order to enable the Data Providers to assess the risks to the rights and freedoms of the Data subjects and the actions required to resolve the issue in accordance with the Privacy and Data Protection Legislation and guidelines.
- 11.2 In case the Personal Data Breach **is likely to result in a high risk** to the rights and freedoms of the Data Subjects, the Data Recipients shall provide full assistance in order for the Data Providers to notify their Supervisory Authority **within 72 hours**, and if required, to notify the affected Data Subjects. Taking into account the conditions of the breach and the security measures applied, the Supervisor Authority might decide that a communication of the breach to the Data Subjects, in line with Article 34 of the GDPR, is not required.
- 11.3 The Data Recipients shall assist the Data Providers to **document** any Personal Data Breaches, comprising the facts relating to the security breaches, its effects and the remedial action taken to enable the Supervisory Authority to verify compliance with Article 33 of the GDPR.

12. DOCUMENTATION OF COMPLIANCE AND AUDIT RIGHTS

- 12.1 Upon request by the Data Providers, the Data Recipients shall make available to the Data Providers all relevant information needed to demonstrate that they are all meeting the requirements of the GDPR, and reasonably cooperate with audits, including inspections by the Data Providers or a competent Supervisory Authority. In order to be able to demonstrate compliance the Parties shall maintain appropriate **records** as described in Clauses 7.6 and 11.3.
- 12.2 The Data Providers shall give notice of any audit or inspection to be conducted to a Data Recipient and shall make reasonable endeavours to avoid causing damage or disruption to the Data Recipients' premises, equipment and work in the course of such an audit or inspection.

12.3 The Data Recipients must inform immediately the Data Providers in case they think they have been given an instruction which does not comply with the Privacy and Data Protection Legislation.

13. TERMINATION

13.1 The Parties agree that following expiration or termination of this Agreement, the Data Recipients shall, **at the choice** of the Data Providers, return all the Personal Data transferred and the copies thereof to the Data Providers or shall destroy all the personal data and certify to the Data Provider that they have done so, unless legislation imposed upon a Data Recipient prevents them from returning or destroying all or part of the Personal Data transferred. In that case, the Data Recipients engaged must warrant that they shall guarantee the confidentiality of the personal data transferred and shall not actively process the personal data transferred anymore. The terms of this Agreement will continue to apply to such Personal Data.

13.2 The Data Providers reserve the right to issue instructions to be followed by the Data Recipients including for the destruction of the Personal Data shared under Clause 13.1, **at any time**.

14. LIMITATION OF LIABILITY

14.1 Nothing in this Agreement relieves the Data Providers and Data Recipients as Joint Controllers of their own direct responsibilities and liabilities under the GDPR.

15. SEVERANCE

15.1 If any provision or part-provision of the **Agreement** is or becomes invalid, illegal or unenforceable, it shall be deemed modified to the minimum extent necessary to make it valid, legal and enforceable. If such modification is not possible, the relevant provision or part-provision shall be deemed deleted. Any modification to or deletion of a provision or part-provision under this clause shall not affect the validity and enforceability of the rest of this agreement.

16. CHANGES TO THE APPLICABLE LAW

16.1 In case the applicable data protection and ancillary laws change in a way that the Agreement is no longer adequate for the purpose of governing lawful data sharing exercises, the Data Providers reserve the right to amend this Agreement. In such circumstances, the Data

Recipients agree to implement any changes to its processing activities as are necessary to comply with the amended terms of the Agreement.

17. FORCE MAJEURE

18.1 Neither Party shall be in breach of this Agreement nor liable for delay in performing, or failure to perform, any of its obligations under this Agreement if such delay or failure results from events, circumstances or causes beyond its reasonable control. In such circumstances the affected party shall be entitled to a reasonable extension of the time for performing such obligations. If the period of delay or non-performance continues for 3 months, the Party not affected may terminate this Agreement by giving 30 days' written notice to the affected Party.

18. GOVERNING LAW AND DISPUTE RESOLUTION

19.1 In case of a dispute between a Data Provider and Data Recipient, the law of the Member State in which the Data provider is established shall govern the Clauses. The Parties will seek to resolve any disputes arising in connection with this Agreement by amicable settlement. The Parties shall abide by a decision of a competent court or of the Lead Supervisory Authority of the Data Provider's country of establishment.

Schedule 1 – Purposes

CARDIOCARE is an international clinical research project. The project is an interdisciplinary collaboration aiming to improve the monitoring, treatment and overall care provided to the elderly breast cancer patients which are at higher risk of developing cardiac toxicity from cancer therapy. Already available **retrospective data from other projects** and data collected within a new **prospective clinical study** will be used for the development and validation of a novel Risk Stratification model for the elderly breast cancer patients.

For the **scientific research purposes** of the Project set under the EC Grant Agreement No 945175, the parties UOI, IEO, BOCOC, KSBC, IOL and NKUA acting as **Data Providers** shall share:

- I. Patients' data available from other projects (where applicable).
- II. Newly collected data from patients enrolled in the CARDIOCARE prospective clinical study.

More specifically, **pseudonymised** data shall be transferred to parties acting as **Data Recipients** to carry out their tasks set under the EC Grant Agreement.

Cloud data processing services including **data transfers and storage** shall be performed using a **Private Cloud infrastructure** provided by **FORTH**, acting as a **Data Recipient** and **Joint Controller**.

Schedule 2 – Description of Personal Data

For the scientific research purposes of the Project described under the EC Grant Agreement the **Data Providers** shall share:

- I. **Pseudonymized** patient data available from other projects including the following **special category/sensitive data**:
 - a. Clinical data
 - b. Cardiac imaging
 - c. Serum biomarkers and psycho-markers (where applicable),
 - d. Blood tests/samples,
 - e. Quality of Life data (where applicable),
 - f. Breast imaging and tissue data

- II. **Pseudonymized** newly collected data from patients enrolled in the CARDIOCARE prospective clinical study including the following **special category/sensitive data**:
 - a. Clinical data
 - b. Cardiac imaging
 - c. Serum biomarkers and psycho-markers,
 - d. Multi-omics (genomics, epigenomics, metagenomics) data
 - e. Quality of Life data
 - f. Intrinsic (mental and physical) capacity monitoring data including wearable sensor and mobile Health application data. Such data collection involves also '**Profiling**' of patients with automated processing of personal data in order to monitor aspects of patients' health, behaviour, location and movements. However, such 'Profiling' **DOES NOT** involve automated individual decision-making, with legal or similarly significant effects for the patients.

Schedule 3 – Description of the Security Measures

Data sharing between the Parties shall be performed using the Private Cloud infrastructure provided by FORTH. The Parties shall implement appropriate technical and organisational security measures to protect the Personal Data shared under the Agreement, including but not limited to:

1. **Pseudonymisation** of the personal data or biological samples by the Data Providers, before uploading the data to the cloud for transferring and/or further processing. The key codes shall be kept in separate location from the Personal Data.
2. **Encryption** of the Personal Data stored within the cloud, to prevent unauthorised and unlawful processing, including Password Storage Encryption, Data Partition Encryption and SSL Host Authentication. Secure and separate access to each Joint Controller shall be provided only upon entering into this Agreement.
3. Appropriate **back-up procedures** in order to avoid accidental loss, destruction or damage of the Personal Data by a physical or technical incident, enabling to reinstate the system in a timely manner.
4. **Secure biological sample storage** conditions including equipment maintenance and authorised processing of the samples by trained personnel only, in order to avoid accidental loss, destruction or damage of the biological samples by a physical or technical incident.
5. **Audit Log operation** to allow viewing the users' access history to the system enabling the detection of any potential security or data breaches.
6. Conducting **regular security assessments** on systems to review the effectiveness of the security measures and on biological sample storage conditions.
7. Ensuring that **pseudonymised** personal data will **not be stored outside the EEA**.
8. Ensuring all research personnel have been made aware of their responsibilities concerning the handling of Personal Data only under the instructions laid down in this Agreement and commit to a duty of confidence by signing a **non-disclosure declaration**.

SIGNATURES

AS WITNESS:

Each person signing below and each Party on whose behalf such person executes this Agreement warrants that he/she, as the case may be, has the authority and the legal capacity to enter into this Agreement and perform the obligation herein.

The Parties have caused this Data Sharing Agreement to be duly signed by the undersigned authorised representatives **in separate signature pages the day and year first above written.**

PANEPISTIMIO IOANNINON (UOI)

Signature:

Name: Prof. Spyridon Georgatos

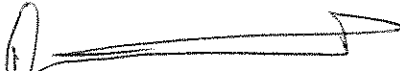
Position: Vice Rector of University of Ioannina

Date:


P.P.
Kikotenni Anton
Vice President



OGKOLOGIKO KENTRO TRAPEZAS KYPROU (BOCOC)

Signature(s) 

Name(s) PANOS ERGATOUDES

Title(s) CHIEF EXECUTIVE OFFICER

Date 14/09/2021

ONKOLOSKI INSTITUT LJUBLJANA (IOL)

Signature(s)

Name(s) **Andreja Uštar, B.Econ.**

Title(s) **Director General**

Date

17 -09- 2021



ERIDPG-0047/2021

ELLINIKO MESOGEIAKO PANEPISTIMIO (HMU)

Signature(s)



Name(s) Manolis Tsiknakis

Title(s) Professor

Date 9/9/2021

CARDIOCARE - Privacy Notice

Version v1.0



Last Updated: October 20th, 2021

This document was drafted pursuant to art. 13 and 14 of EU General Data Protection Regulation 2016/679 (hereafter: "GDPR") in order to let you know our privacy policy and to understand how your personal data is being handled for the scientific research purposes of the CARDIOCARE project (hereinafter "Project"). The general information published on this page is intended to supplement the information that has been given to data subjects (for example on a participant information sheet or a consent form) when collecting their personal data to allow them to exercise their rights.

1. Purposes of the processing

CARDIOCARE has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 945175, entitled: "AN INTERDISCIPLINARY APPROACH FOR THE MANAGEMENT OF THE ELDERLY MULTIMORBID PATIENT WITH BREAST CANCER THERAPY INDUCED CARDIAC TOXICITY". The Project is a collaborative effort from leading scientists in 7 countries across Europe (Greece, Italy, Cyprus, Slovenia, Sweden, Netherlands, and France). CARDIOCARE is aiming to improve the monitoring, treatment and overall care provided to the **elderly breast cancer patients** which are at high risk of developing cardiac toxicity from cancer therapy.

More specifically, aged-related factors and co-morbidities increase elderly breast cancer patients' vulnerability to cardiotoxicity due to cancer treatment. CARDIOCARE will focus on the elderly breast cancer population and through a holistic approach including mobile Health applications, wearable sensors and biomarkers, will provide the ability to patients to take part in their care process and enhance their physical and mental health, contributing to an individualized care plan and a psychological adaptation to their disease. CARDIOCARE will enable the development of an effective risk stratification model in mitigating cardiotoxicity and adverse events, minimizing hospitalisations and enhancing quality of life.

2. About the Data Controller

The organisation which is collecting and processing your personal data, is the

- PANEPISTIMIO IOANNINON (UOI), established in PANEPISTEMIOYPOLE
PANEPISTEMIO IOANNINON, IOANNINA 45110, Greece.

For the scientific research purposes of the project, UOI (hereinafter "Data Provider") will provide **non-identifiable data (pseudonymised data)** to other CARDIOCARE research partners, all acting as Joint Controllers.

If you have any questions about the particular research study you are participating in, please use any contact details you have already been supplied with or feel free to contact us at

For any information concerning the processing of your personal data by UOI, you can contact the Data Protection Officer at the following address: dpo@uoi.gr

3. About the personal data we process

For the medical research purposes of CARDIOCARE, UOI will process:

- (i) Pseudonymized patient data available from other projects or registries.

- (ii) Newly collected data from patients enrolled in the CARDIOCARE prospective clinical study

The types of personal data that shall be processed for the purposes of the project include clinical data, cardiac imaging, serum biomarkers, multi-omics (genomics, epigenomics) data, Quality of Life data and intrinsic (mental and physical) capacity monitoring data including wearable sensor and mobile Health application data.

The types of processing activities planned for the project include clinical, biochemical, molecular biology, biomedical imaging, machine learning and statistical modelling approaches together with wearable sensor and mHealth applications technologies involving cloud services and information security technologies. Such data processing involves also 'Profiling' of patients with automated processing of personal data in order to monitor aspects of patients' health, behaviour, location and movements. However, such 'Profiling' DOES NOT involve automated individual decision-making, with legal or similarly significant effects for the patients.

4. Legal basis for the processing

- (i) For the purposes of further processing patients' data available from other projects or registries, lawful processing is based on the following legal grounds:
 - a. Processing is necessary for the performance of a task carried out in the public interest according to Article 6(1e) of the GDPR. The task or function has a clear basis in law in line with Recital 45 of the GDPR. For non-public bodies, processing is necessary for the legitimate interests in scientific research pursued by the Project participants according to Article 6(1f) of the GDPR.
 - b. Further processing is based on scientific research purposes as a lawful compatible purpose, in line with Recitals 50 and 159 of the GDPR.
 - c. Additional condition for processing sensitive / special category data including health data is that processing is necessary for scientific research purposes in the public interest and in the area of public health according to Article 9(2j) and Recitals 52, 53 and 159 with appropriate safeguards in line with Article 89(1) and Recitals 156 and 157 of the GDPR.
- (ii) For the purposes of processing newly collected data from patients enrolled to the CARDIOCARE prospective clinical study, lawful processing is based on the following legal grounds:
 - a. Lawful Processing is necessary for the performance of a task carried out in the public interest according to Article 6(1e) of the GDPR. The task or function has a clear basis in law in line with Recital 45 of the GDPR. For non-public bodies, processing is necessary for the legitimate interests in scientific research pursued by the beneficiaries according to Article 6(1f) of the GDPR.
 - b. Additional condition for processing sensitive / special category data including health data is that processing is necessary for scientific research purposes in the public interest and in the area of public health according to Article 9(2j) and Recitals 52, 53 and 159 with appropriate safeguards in line with Article 89(1) and Recitals 156 and 157 of the GDPR.

You are not legally or contractually obliged to supply us with your personal information for research purposes.

5. Data subject rights

Various rights under GDPR, including the right to access personal information that is held about you, are qualified or do not apply when personal data is processed solely in a scientific research

context. This is because fulfilling them might adversely affect the integrity of, and the public benefits arising from the clinical research study. For this reason,

- (i) As far as the processing of data available from other projects or registries based on the legal grounds described above, the Data Subjects are entitled to the following rights:
 - a. The right to be informed, the right of access and the right to rectification.
Based on the specific legal grounds for processing, the rights to erasure, to data portability, and to object are NOT available in line with Recital 65 and Article 17(3d), Recital 68, and Article 21(6) plus Recital 159 of the GDPR respectively.
- (ii) As far as the processing of newly collected data from patients enrolled to the CARDIOCARE prospective clinical study, based on the legal grounds described above, the Data Subjects are entitled to the following rights:
 - a. The right to be informed, the right of access and the right to rectification.
Based on the specific legal grounds for processing, the rights to erasure, to data portability, and to object are NOT available in line with Recital 65 and Article 17(3d), Recital 68, and Article 21(6) plus Recital 159 of the GDPR respectively.

6. The recipients of the pseudonymized data

For the scientific research purposes of the CARDIOCARE project, UOI (Data Provider) will share pseudonymized personal data to the following European Economic Area (EEA)-based Data Recipients, acting as Joint Data Controllers:

- ISTITUTO EUROPEO DI ONCOLOGIA SRL (IEO), established in Via Filodrammatici 10, MILANO 20121, Italy.
- OΓKOΛOΓIKO KENTPO TPAPEZAS KYPROU (BOCOC), established in LEOFOROS AKROPOLEOS 32, STROVOLOS 2006, Cyprus.
- IDRYMA TECHNOLOGIAS KAI EREVNAS (FORTH), established in N PLASTIRA STR 100, IRAKLEIO 70013, Greece.
- PHILIPS ELECTRONICS NEDERLAND BV (PHILIPS), established in HIGH TECH CAMPUS 52, EINDHOVEN 5656 AG, Netherlands.
- KAROLINSKA UNIVERSITY HOSPITAL (KSBC), established in HANTVERKARGATAN 45, STOCKHOLM 104 22, Sweden.
- STREMBLE VENTURES LTD (STREMBLE), established in KO 8 GERMASOGEIA, LIMASSOL 4045, Cyprus.
- ONKOLOSKI INSTITUT LJUBLJANA (IOL), established in ZALOSKA CESTA 2, LJUBLJANA 1000, Slovenia.
- ETHNIKO KAI KAPODISTRIAKO PANEPISTIMIO ATHINON (NKUA), established in 6 CHRISTOU LADA STR, ATHINA 10561, Greece.
- ELLINIKO MESOGEIAKO PANEPISTIMIO (HMU), established in ESTAVROMENOS, HERAKLION 71004, Greece.

in order to carry out the tasks described under EU Grant Agreement No 945175.

The Personal Data shall be transferred using a Private Cloud infrastructure provided by FORTH, a CARDIOCARE partner acting as a Data Recipient and Joint Controller.

7. Data retention

The Data Provider will retain the personal data as long as needed for scientific research purposes in line with Article 5(1e) and in accordance with Article 89(1) of the GDPR subject to appropriate technical and organizational measures to safeguard the rights and freedoms of the data subjects.

At the end of the project (for a minimum of 4 years, unless an extension is granted by the European Commission) and at the choice of the Data Provider, the Data Recipients shall return or destroy all the Personal Data transferred.

8. Right to lodge a complaint

If you believe that the processing of your personal data is not performed in a GDPR compliant manner, you are always entitled to lodge a complaint to the Supervisory Authority at <https://www.dpa.gr/>.

9. Changes made to this webpage.

This webpage was last updated on October 20th, 2021. It is reviewed when necessary and at least annually. Any changes will be published here.

Data Protection Impact Assessment (DPIA)

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the [Criteria for an acceptable DPIA](#) set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	PANEPISTIMIO IOANNINON (UOI), established in PANEPISTEMIOYPOLE PANEPISTEMIO IOANNINON, IOANNINA 45110, Greece
DPIA subject	Identify and minimize any data protection risks related to the EU’s Horizon 2020 project: “CARDIOCARE- AN INTERDISCIPLINARY APPROACH FOR THE MANAGEMENT OF THE ELDERLY MULTIMORBID PATIENT WITH BREAST CANCER THERAPY INDUCED CARDIAC TOXICITY”.
Name of controller contact	Professor Dimitris Fotiadis, Head of the Unit of Medical Technology and Intelligent Information Systems, Department of Materials Science and Engineering, University of Ioannina, Greece Email: dimitris.fotiadis30@gmail.com, Tel: +302651009006

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarize why you identified the need for a DPIA.

UOI is the Coordinator of and partner in the CARDIOCARE project. The project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 945175, entitled: "AN INTERDISCIPLINARY APPROACH FOR THE MANAGEMENT OF THE ELDERLY MULTIMORBID PATIENT WITH BREAST CANCER THERAPY INDUCED CARDIAC TOXICITY".

CARDIOCARE is an interdisciplinary clinical research project. The project is an international collaboration aiming to improve the monitoring, treatment and overall care provided to the elderly breast cancer patients which are at higher risk of developing cardiac toxicity from cancer therapy. Already available retrospective data from other projects and data collected within a new prospective clinical study will be used for the development and validation of a novel Risk Stratification model for the elderly breast cancer patients.

For the scientific research purposes of the project set under the Grant Agreement No 945175, UOI will be one of the six clinical centres of the study and acting as a **Joint Controller** (Data Provider), will share the following of data:

- I. Patient data already available from other projects.
- II. Newly collected data from patients enrolled in the CARDIOCARE prospective clinical study.

The types of personal data that shall be shared for the purposes of the project include clinical data, cardiac imaging, serum biomarkers and psycho-markers, multi-omics (genomics, epigenomics) data, Quality of Life data and intrinsic (mental and physical) capacity monitoring data including wearable sensor and mobile Health application data. Such data processing involves also 'Profiling' of patients with automated processing of personal data in order to monitor aspects of patients' health, behaviour, location and movements. However, such 'Profiling' DOES NOT involve automated individual decision-making, with legal or similarly significant effects for the patients.

Considering the **special category/sensitive nature** of the personal data that shall be processed, comprising health and genetic data, as well as the requirement to transfer such data to other CARDIOCARE partners (**Data Recipients**) for processing, a need for a DPIA is identified in accordance with Article 35 (3b) of the GDPR. This DPIA is performed in order to assess any potential risks arising from the processing activities planned and to assess the effectiveness of the technical and organisational measures taken for the protection of the rights and freedoms of the data subjects.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

In order for the partners to carry out the tasks set under the project's Grant Agreement No 945175, transfers of patient data are necessary between the partners. The partners, as **Joint Controllers** will enter an appropriate **Data Sharing Agreement** in line with Article 26(1) of the GDPR. For the research purposes of the project, UOI acting as a **Data Provider** shall share:

- I. Patient data already available from other projects.
- II. Newly collected data from patients enrolled in the CARDIOCARE prospective clinical study.

More specifically, **pseudonymised** data shall be transferred to Joint Controllers acting as **Data Recipients** to carry out their tasks set under the EC Grant Agreement.

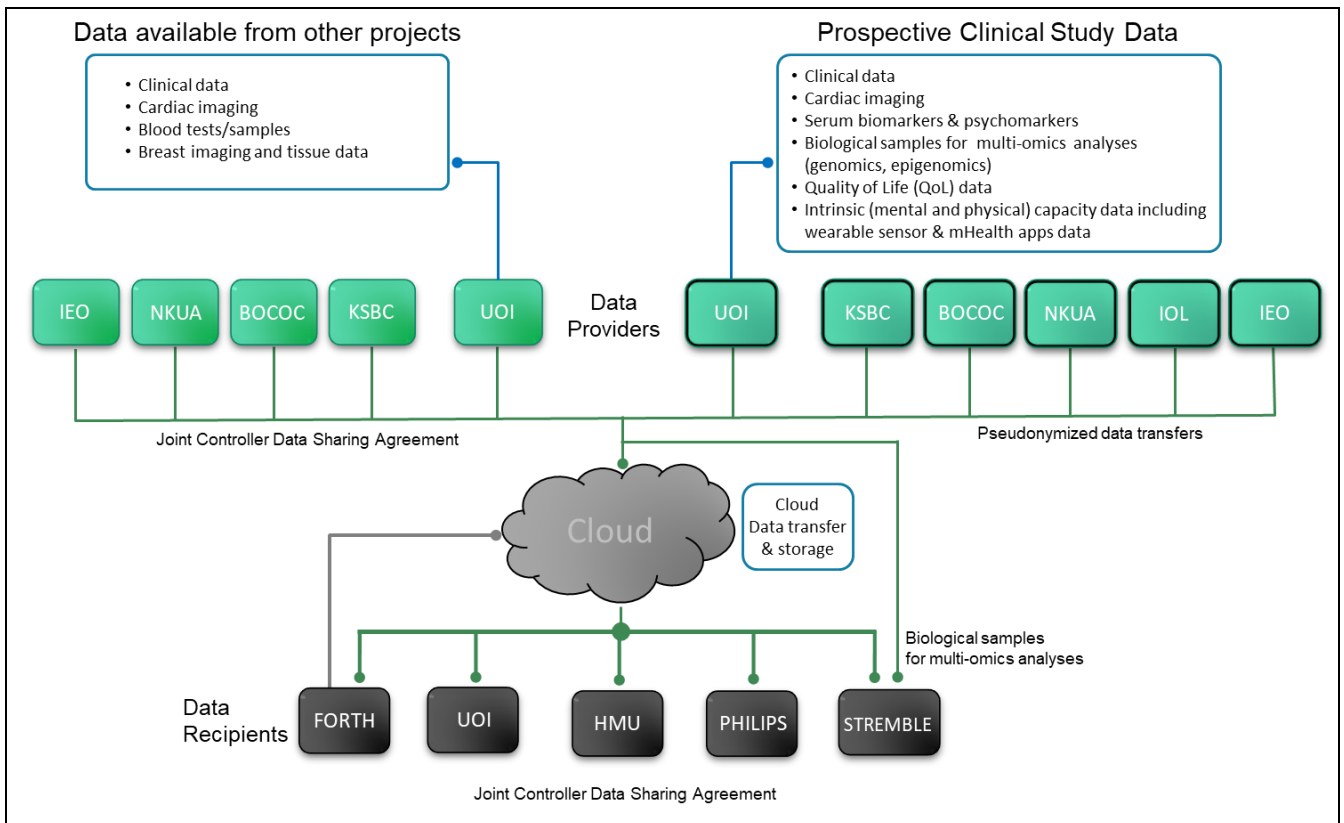
Cloud data processing services including **data transfers and storage** shall be performed using a **Private Cloud infrastructure** provided by the CARDIOCARE partner **FORTH**, acting as a Data Recipient and **Joint Controller**.

The Data Provider will retain the personal data as long as needed for scientific research purposes in line with Article 5(1e) and in accordance with Article 89(1) of the GDPR subject to appropriate technical and organizational measures to safeguard the rights and freedoms of the data subjects.

At the end of the project (for a minimum of 4 years, unless an extension is granted by the European Commission) and at the choice of the Data Provider, the Data Recipients shall return or destroy all the Personal Data transferred, unless legislation imposed upon them prevents them from returning or destroying all or part of the personal data transferred.

Taking into account the special category nature of the data that shall be processed and the requirement to transfer such data to partners in other countries for further processing, via a cloud infrastructure, appropriate technical and organisational measures are needed to mitigate any risks arising from such types of processing activities that involve a likely high risk for the rights and freedoms of the data subjects.

Collectively, the data flows are described in the following diagram.



Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

For the research purposes of the project UOI shall share the following patient data collected by the Department of Medical Oncology (Prof. Davide Mauri) and the 2nd Department of Cardiology (Prof. Katerina Naka) at the University Hospital of Ioannina in Greece:

- I. **Pseudonymized** data from **100 patients** available from other projects including the following **special category/sensitive data**:
 - a. Clinical data
 - b. Cardiac imaging
 - c. Blood tests/samples
 - d. Breast imaging and tissue data
- II. **Pseudonymized** newly collected data from **60 patients** enrolled in the CARDIOCARE prospective clinical study including the following **special category/sensitive data**:
 - a. Clinical data
 - b. Cardiac imaging
 - c. Serum biomarkers and psycho-markers

- d. Biological samples for multi-omics analyses (genomics, epigenomics)
- e. Quality of Life data
- f. Intrinsic (mental and physical) capacity monitoring data including wearable sensor and mobile Health application data. Such data processing involves also '**Profiling**' of patients with automated processing of personal data in order to monitor aspects of patients' health, behaviour, location and movements. However, such 'Profiling' **DOES NOT** involve automated individual decision-making, with legal or similarly significant effects for the patients.

The patient data will be retained as long as needed for scientific research purposes in compliance with Article 5(1e) and the Member State's applicable law.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

The relationship with the data subjects is characterized as patient – doctor relationship and as research participant in nature, where the patient is expecting the use of its health data for scientific research purposes in the area of Breast Cancer and Cardio-Oncology research. UOI as a Joint Controller and Data Provider ensures that the personal data will be lawfully processed for the public good and for legitimate research activities while protecting the interests of the data subjects. In addition, the Data Provider ensures the processing of personal data to be both fair and transparent in order for the patients to retain control over their personal data. For this reason, the Data Provider undertakes to inform, where applicable, the data subjects with the information listed in Articles 13 and 14 of the GDPR in order to comply with the principles of fairness and transparency.

The data concern elderly breast cancer patients. No children or other vulnerable groups are included as research participants.

The types of processing activities planned for the project include clinical, biochemical, molecular biology, biomedical imaging, machine learning and statistical modelling approaches together with wearable sensor and mHealth applications technologies involving cloud services and information security technologies. No approved code of conduct or certification scheme exists, yet.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Aged-related factors and co-morbidities increase elderly breast cancer patients' vulnerability to cardiotoxicity due to cancer treatment. Lack of best practices and frailty bias in these patients, underrepresented in clinical trials, may lead to inappropriate interventions and undertreatment, resulting in poorer outcomes, deterioration of quality of life and increased healthcare costs. CARDIOCARE will focus on the elderly breast cancer population and through a holistic approach including mHealth applications, wearable sensors, imaging and molecular biomarkers, will provide the ability to patients to take part in their care process and enhance their physical and mental health (intrinsic capacity), contributing to an individualised care plan and a psychological adaptation to their disease. CARDIOCARE will enable the development of an effective risk stratification model in mitigating cardiotoxicity and adverse events, minimizing hospitalisations and enhancing quality of life.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

EUROPA DONNA – The European Breast Cancer Coalition is an international breast cancer patient advocacy organization which has endorsed the CARDIOCARE project and will participate in the **Ethical Advisory Board** and the **Regulatory Advisory Board** of the project.

This endorsement can be mutually beneficial by encouraging patients' participation to the management of their condition while assisting the medical experts to get a deeper understanding of patients' concerns and expectations regarding their health and the protection of their personal data.

EUROPA DONNA will help communicate the project's results and advise on ethical, privacy, health and quality of life issues concerning breast cancer patients. In addition EUROPA DONNA will help highlight the need for early diagnosis of cardiotoxicity after cancer treatment, inform about care and treatment choices available to improve mental and physical health and QoL, and encourage patients to have an active role in decisions regarding their own health.

The endorsement of the EUROPA DONNA to the CARDIOCARE project is provided below:



President
M. Elzayat
Austria

Vice President
T. Spanic
Slovenia

Treasurer
S. Erdem
Turkey

E. Bergsten-Nordström
Sweden

B. Dodeva
North Macedonia

P. Mosconi
Italy

F. Poulakaki
Greece

V. Ramljak
Croatia

E. Verschuur
The Netherlands

Executive Director
S. Knox

To: Prof. Dimitrios I. Fotiadis, Coordinator of the CARDIOCARE consortium

Date: May 18, 2020

Reference:

Subject: Support of the CARDIOCARE research proposal for the H2020 call SC1-BHC-24-2020: Healthcare interventions for the management of the elderly multimorbid patient.

Dear Prof. Dimitrios I. Fotiadis,

Concerning your research proposal entitled "CARDIOCARE - AN INTERDISCIPLINARY APPROACH FOR THE MANAGEMENT OF THE ELDERLY MULTIMORBID PATIENT WITH BREAST CANCER THERAPY INDUCED CARDIAC TOXICITY".

We are pleased to inform you that EUROPA DONNA - The European Breast Cancer Coalition, an independent non-profit organisation representing the interests of European women regarding breast cancer, will support your efforts in case the proposal is accepted for funding, in terms of participating in the advisory board. EUROPA DONNA member(s) will advise on ethical, privacy, health and quality of life issues concerning breast cancer patients. All costs for the participation of the EUROPA DONNA member(s) to the advisory board meetings, including any travelling expenses, will be covered by the CARDIOCARE consortium.

We hope for a positive decision for funding this project.

Sincerely,

Susan Knox
CEO/Executive Director

Founding President
G. Freilich

Founder
Prof. U. Veronesi

Head Office: Piazza Amendola, 3 - 20149 Milan, Italy - Tel. +39-02.3659 2280 - Fax +39-02. 3659 2284 - E-mail info@europadonna.org
www.europadonna.org

In addition, the medical associations European Society of Cardiology (ESC), a CARDIOCARE partner and the International Cardio-Oncology Society (ICOS) which has also endorsed the project, will have an active role by advising on ethical issues concerning the protection of the patients' data.

All Data Recipients have provided all available information to perform this Data Protection Impact Assessment.

All research staff handling personal data has been made aware of its responsibilities with regards to handling of Personal Data and will commit to a duty of confidence by signing a non-disclosure declaration.

Information Security issues have been addressed by FORTH, a CARDIOCARE technical partner leader of the relevant "**Task 5.3: The CARDIOCARE Security tools and services**".

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

For the purposes of **further processing** patients' data available from other projects (I), lawful processing is based on the following legal grounds:

- a. Processing is necessary for the **performance of a task carried out in the public interest** according to Article 6(1e) of the GDPR. The task or function has a clear basis in law in line with Recital 45 of the GDPR. For non-public bodies, processing is necessary for the **legitimate interests in scientific research** pursued by the beneficiaries according to Article 6(1f) of the GDPR.
- b. Further processing is based on **scientific research purposes** as a lawful compatible purpose, in line with Recitals 50 and 159 of the GDPR.
- c. Additional condition for processing sensitive / special category data including health data is that processing is necessary for **scientific research purposes in the public interest and in the area of public health** according to Article 9(2j) and Recitals 52, 53 and 159 with appropriate safeguards in line with Article 89(1) and Recitals 156 and 157 of the GDPR.

For the purposes of processing newly collected data from patients enrolled to the CARDIOCARE prospective clinical study (II), lawful processing is based on the following legal grounds:

- a. Processing is necessary for the **performance of a task carried out in the public interest** according to Article 6(1e) of the GDPR. The task or function has a clear basis in law in line with Recital 45 of the GDPR. For non-public bodies, processing is necessary for the **legitimate interests in scientific research** pursued by the beneficiaries according to Article 6(1f) of the GDPR.
- b. Additional condition for processing sensitive / special category data including health data is that processing is necessary for **scientific research purposes in the public interest and in the area of public health** according to Article 9(2j) and Recitals 52, 53 and 159 with appropriate safeguards in line with Article 89(1) and Recitals 156 and 157 of the GDPR.

For the purposes described above the Data Provider (UOI) undertakes to inform, where applicable, the data subjects with the **information listed in Articles 13 and 14** of the GDPR in order to comply with the principle of **transparency**.

As far as the further processing of patient data available from other projects (I), based on the legal grounds used, the Data Subjects are entitled to the following **rights**:

- a. The right to be informed, the right of access and the right to rectification.
- b. Based on the specific legal grounds for processing, the rights to erasure, to data portability, and to object are **NOT** available in line with Recital 65 and Article 17(3d), Recital 68, and Article 21(6) plus Recital 159 of the GDPR respectively.

As far as the processing of newly collected data from patients enrolled to the CARDIOCARE prospective clinical study (II), based on the legal grounds used, the Data Subjects are entitled to the following **rights**:

- a. The right to be informed, the right of access and the right to rectification.
- b. Based on the specific legal grounds for processing, the rights to erasure, to data portability, and to object are **NOT** available in line with Recital 65 and Article 17(3d), Recital 68, and Article 21(6) plus Recital 159 of the GDPR respectively.

Data Subjects can exercise their rights through a Subject Access Request to the Data Provider. To facilitate the Data Subjects' rights, the Data Provider and Data Recipients shall maintain Records of all Personal Data processed and all processing activities in a structured, commonly used and machine-readable form in accordance with Article 30 of the GDPR.

Data transfers between Joint Controllers shall be performed using the **Cloud infrastructure** provided by FORTH (an EU-based partner) acting as a Data Recipient and Joint Controller.

Considering the risks arising from the processing activities involved, the Joint Controllers shall implement strategies of **data protection by design** including appropriate technical and organisational measures to ensure data quality and minimisation and a level of security appropriate to those risks, including but not limited to:

1. **Pseudonymisation** of the personal data or biological samples by the Data Providers, before uploading the data to the cloud for transferring and/or further processing. The key codes shall be kept in separate location from the Personal Data.
2. **Encryption** of the Personal Data stored within the cloud, to prevent unauthorised and unlawful processing, including Password Storage Encryption, Data Partition Encryption and SSL Host Authentication. Secure and separate access to each joint controller shall be provided only upon entering into this Agreement.
3. Appropriate **back-up procedures** in order to avoid accidental loss, destruction or damage of the Personal Data by a physical or technical incident, enabling to reinstate the system in a timely manner.
4. **Secure biological sample storage** conditions including equipment maintenance and authorised processing of the samples by trained personnel only, in order to avoid accidental loss, destruction or damage of the biological samples by a physical or technical incident.
5. **Audit Log operation** to allow viewing the users' access history to the system

enabling the detection of any potential security or data breaches.

6. Conducting **regular security assessments** on systems to review the effectiveness of the security measures and on biological sample storage conditions.
7. Ensuring that pseudonymised personal data will **not be stored outside the European Economic Area (EEA)**.
8. Ensuring all research personnel have been made aware of their responsibilities concerning the handling of Personal Data only under the instructions laid down in this Agreement and commit to a duty of confidence by signing a **non-disclosure declaration**.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm Remote, possible or probable	Severity of harm Minimal, significant or severe	Overall risk Low, medium or high
<p>1. Impossible or disproportionate effort to directly inform the data subjects of the further processing operations.</p> <p>For the purposes of further processing patients’ data available from other projects (I), the Data Provider shall provide the data subjects concerned, and where applicable, with Article 13 and 14 information regarding that further processing operation.</p> <p>Considering that the processing is carried out for scientific research purposes involving a large number of data subjects, data of a certain age, and likely a number of no more valid contact details it might be impossible or involve a disproportionate effort to directly inform the data subjects of that further processing (GDPR Recital 62), in order to enable them to exercise their rights.</p> <p>However, taking into account the compatible nature of further processing for scientific research purposes, the pseudonymization of the personal data by the Data Provider and the existence of appropriate safeguards (see, pages 9-10) in the intended further</p>	Probable	Minimal	Medium

processing operations, the overall risk for the data subjects is considered medium .			
<p>2. Illegitimate access to data.</p> <p>Considering the technical and organisational security measures applied (see, pages 9-10), including but not limited to data pseudonymization, encryption, secure and separate access under an Article 26(1) data sharing agreement and an Article 28 contract, the overall risk for the data subjects is considered low.</p>	Remote	Minimal	Low
<p>3. Undesired modification of data</p> <p>Considering the technical and organisational security measures applied (see, pages 9-10), including but not limited to the commitment of the authorized research personnel to a duty of confidence by signing a non-disclosure declaration, the overall risk for the data subjects is considered low.</p>	Remote	Minimal	Low
<p>4. Disappearance of data.</p> <p>Taking into account that the personal data shall be pseudonymised before uploaded to the Cloud, stored encrypted and systematically backed-up in external RAID drives the overall risk for the data subjects is considered Low.</p>	Possible	Minimal	Low
<p>5. Breach of any Data Recipient's obligation to protect the personal data of the data subjects.</p> <p>Considering that the recipients of the pseudonymised data are partners in the CARDIOCARE project under EC Grant Agreement No 755320 and that an appropriate Article 26(1) Data Sharing Agreement for Joint Controllers is in place, the overall risk is considered Low.</p>	Remote	Minimal	Low
<p>6. Patient 'Profiling' involving tracking or observation of participants.</p> <p>Intrinsic capacity monitoring includes wearable sensor and mobile Health application data processing. Such processing involves also 'Profiling' of patients with automated processing of data in order to</p>	Remote	Minimal	Low

<p>monitor aspects of patients' health, behaviour, location and movements. However, such 'Profiling' DOES NOT involve automated individual decision-making, with legal or similarly significant effects for the patients. Taking into account the technical and organisational security measures applied (see, pages 9-10), the overall risk for the data subjects is considered low.</p>			
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as <u>medium</u> or <u>high</u> risk in step 5				
Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
		Eliminated reduced accepted	Low medium high	Yes/no
1. Impossible or disproportionate effort to directly inform the data subjects of the further processing operations, in order to enable them to exercise their rights.	Making the required information, about further processing operations, publicly available through the Data Provider's website (as a Privacy Notice).	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Prof. Dimitrios I. Fotiadis / 09-12-2021	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the DPA before going ahead

DPO advice provided:	UOI DPO (dpo@uoi.gr) 09-12-2021	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: The processing can proceed. Data protection obligations have been met and no further measures are required.		
DPO advice accepted or overruled by:	Prof. Dimitrios I. Fotiadis / 09-12-2021	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	Michalis D. Mantzaris	The DPO should also review ongoing compliance with DPIA



9-12-2021

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ ΠΡΥΤΑΝΕΙΑ

Α.Π: 1

ΥΠΗΡΕΣΙΑ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Προς τον κ. Δημήτριο Φωτιάδη,
Καθηγητή Τμήματος Μηχανικών
Επιστήμης Υλικών
Πανεπιστημίου Ιωαννίνων

Υ.Π.Δ: Σταυρούλα Σταθαρά
Τηλέφωνο: 26510 07321 e-
mail: dpo@uoi.gr

**ΘΕΜΑ: ΕΓΚΡΙΣΗ ΕΠΕΞΕΡΓΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ**

**ΚΑΙ. ΜΕΛΕΤΗΣ ΕΚΤΗΝΙΗΣΗΣ ΑΝΤΙΚΤΥΠΟΥ (DPIA) ΓΙΑ ΤΟΥΣ
ΕΡΕΥΝΗΤΙΚΟΥΣ ΣΚΟΠΟΥΣ ΤΟΥ ΠΡΟΓΡΑΜΜΑΤΟΣ «CARDIOCARE».**

Αξιότιμε κ. Φωτιάδη,

Σε απάντηση του υποβληθέντος αιτήματος σας , το οποίο αφορά σε έγκριση της ερευνητικής μελέτης με ακρωνύμιο «CARDIOCARE» , στο πλαίσιο του ερευνητικού Προγράμματος με τίτλο « Μια διεπιστημονική προσέγγιση για την διαχείριση της πολυνοσηρότητας ηλικιωμένων ασθενών με καρκίνο του στήθους που εμφανίζουν καρδιοτοξικότητα επαγόμενη από χημειοθεραπεία» με κωδικό έργου Επιτροπής Ερευνών του Πανεπιστημίου Ιωαννίνων (...XXI) και αφού λάβαμε υπόψη μας το περιεχόμενό του, σας ξημερώνουμε ως ακολούθως:

Το υποβληθέν αίτημα εγκρίνεται άνευ παρατηρήσεων, δεδομένου ότι, πληροί τους όρους και τις προϋποθέσεις που ορίζονται για την επεξεργασία δεδομένων προσωπικού χαρακτήρα στις διατάξεις των άρθρων 5 και 6 (ΕΕ) 2016/679 (ΓΚΠΔ) και των άρθρων 5, 24 και 30 του Ν.4624/2019, τα δεδομένα δε που θα συλλεγού, είναι ανωνυμοποιημένα, ώστε να μην υπάρχει δυνατότητα ταυτοποίησης των υποκειμένων των δεδομένων.

Για τον σκοπό της ανωτέρω αναφερόμενης επεξεργασίας, διεξήχθη, σύμφωνα με τα οριζόμενα στο άρθρο 35 παρ (1) (ΕΕ) 2016/679 (ΓΚΠΔ) η απαιτούμενη Μελέτη Εκτίμησης Αντίκτυπου(ΟΡΙΑ), αναφορικά με την εκτίμηση των επιπτώσεων και τους κινδύνους για τα δικαιώματα και τις ελευθερίες των συμμετεχόντων στην έρευνα φυσικών προσώπων, τα αποτελέσματα της οποίας ελήφθησαν υπόψη.

Το Πανεπιστήμιο Ιωαννίνων, ως «υπεύθυνος επεξεργασίας», έχει λάβει τα κατάλληλα τεχνικά και οργανωτικά μέτρα, με σκοπό την διασφάλιση της ακεραιότητας και της εμπιστευτικότητας της επεξεργασίας (παρ. (στ) αρ. 5 (ΕΕ) 2016/679).

Επίσης σας ενημερώνουμε ότι η Υπηρεσία μας, τελεί στη διάθεση σας για οιαδήποτε περαιτέρω διευκρίνιση η πληροφορία.

Με τιμή

Σταυρούλα



Σταθαρα

Υ.Π.Δ. Παν/μιου Ιωαννίνων



Σ Α.Δ ΑΛΝΠΙΑΝΗΣ