Ref. Ares(2025)11362650 - 18/12/2025
Funded by
the European Union

Deliverable D12 (7.1)

GDPR Framework

Grant Agreement number	101137244
Project Acronym	KEEPCARING
Project Full Title	Future Proofing Health- and Care Systems Safeguarding Health Care Workers in Hospital Settings
EU Project Officer	Athanasios Rogdakis
Horizon Europe Call	HORIZON-HLTH-2023-CARE-04
Project duration	48 months
Deliverable	D12 (7.1) - GDPR Framework
Version	V.1
WP	WP7
Lead Beneficiary	CHINO
Authors	Ermanno Pallaoro - Maria Grassetto
Due Date (as in GA)	M18
Actual Submission date	18/12/2025

1. The KEEPCARING project

Healthcare professionals working in hospitals - and those in training to embark on hospital careers - experience high levels of stress, especially in the surgical pathways. While interventions to improve wellbeing and resilience exist, not much is known about the right (combination of) intervention(s) for this specific setting. KEEPCARING aims to (re-)build wellbeing and resilience of healthcare workforce in EU hospitals by co-creating a multi-faceted non-digital, digital and AI-supported solution package to prevent burnout among (aspirant) healthcare professionals on the individual, team, and organizational level. Our multi-sector and interdisciplinary consortium will (1) study stress and stressors experienced by (aspiring) health care providers in their specific setting, (2) evaluate digital and non-digital solutions to reduce stress at an individual and team level, (3) study job crafting among (aspiring) health professionals as a way to reduce stress, and (4) finally, develop a change management platform that, using explainable AI, helps hospital managers as well as surgical caregivers to choose the solutions that match their context. All solutions as well as the portal will be developed in co-creation with end users, including two professional associations in our consortium. In addition, legal and ethical expertise is provided across Partners and in the Advisory Board to ensure privacy and ethical guidance in this sensitive context.

KEEPCARING will provide solutions to improve wellbeing among health care professionals and students, thereby reducing burnout and improving the number of health care students entering the workplace. Our organizational solutions will empower individuals and employers to understand and act on stressful situations in their specific setting. Cost-effectiveness analyses will be used for policy recommendations to ensure sustainable uptake among policy makers, funders, and employers.

ABBREVIATIONS (to be refined)

AI: Artificial Intelligence

AUMC: Amsterdam UMC (Partner - Netherlands)

BDSG: *Bundesdatenschutzgesetz* (German Federal Data Protection Act)

BetrVG: *Betriebsverfassungsgesetz* (German Works Constitution Act)

CHINO: Partner / Lead Beneficiary of WP7

CMP: Change Management Platform

CNR: National Research Council (Partner - Italy)

COO: Coordinator (AUMC)

DMP: Data Management Plan

DPA: Data Processing Agreement (Contract between Controller and Processor)

DPIA: Data Protection Impact Assessment

DPO: Data Protection Officer

DIGITALTWIN: Technical Partner (Successor to NURO)

ECHA: Partner Entity (Mentioned in context of signing a JCA with DIGITALTWIN)

EU: European Union

EUR: Erasmus University Rotterdam (Partner - Netherlands)

GA: Grant Agreement

GDPR: General Data Protection Regulation (EU) 2016/679

HADEA: European Health and Digital Executive Agency (Granting Authority)

HR: Human Resources

INN: Hogskolen i Innlandet (Partner - Norway)

JCA: Joint Controllership Agreement

MVP: Minimum Viable Product

NOVA: Universidade Nova de Lisboa (Partner - Portugal)

NURO: Former Technical Partner (Predecessor to DIGITALTWIN)

OR: Operating Room

ORBB: Operating Room Black Box

PN: Privacy Notice

RIGS: Rigshospitalet (Partner - Denmark)

RoPA: Record of Processing Activities

SST: Surgical Safety Technologies, Inc. (Vendor - Canada)

UAVG: *Uitvoeringswet Algemene verordening gegevensbescherming* (Dutch GDPR Implementation Act)
UKE: University Medical Centre Hamburg-Eppendorf (Partner - Germany)
UL: University of Limerick (Partner - Ireland)
UoC: University of Coimbra (Alternative acronym used in summary tables)
VR: Virtual Reality
WP: Work Package

2. Executive Summary

Last Document Update: 17 December 2025.

This document constitutes **Deliverable D12 (7.1) - GDPR Framework** and serves as the primary governance instrument for managing data protection compliance within the KEEPCARING Project ensuring alignment with the General Data Protection Regulation (EU) 2016/679 (GDPR) and relevant national legislations.

The aim of this document is to ensure that data collection and further use of personal data for the purpose of the research remains at all times compliant with the current legislation, proposing recommendations, defining rules for the relationship between the Partners involved in the different research activities (Studies A through F) and providing guidelines for the technical developments (the Change Management Platform).

This deliverable provides both high-level governance rules and specific operational details:

- **Section 3 (GDPR Compliance):** Defines the data protection and security requirements that must be fulfilled to process personal data lawfully within the project.
- **Section 4 (Data Processing Activities carried out within the Project):** Provides a granular analysis of each research study (A–F) and technical asset from a data protection point of view. This includes the roles of the Partners, the legal basis, data flows, and specific risk for each activity.
- **Section 5 (Summary Tables):** Features the "Action Plan" and status trackers for Privacy Notices, Joint Controllership Agreements (JCAs), and Data Protection Impact Assessments (DPIAs).
- **Section 6 (Annexes):** Houses the current versions of all drafted and executed legal documentation.

3. GDPR Compliance

Since the project involves the collection and processing of personal data of healthcare professionals, the General Data Protection Regulation (EU) 2016/679 (GDPR) constitutes the primary legal framework within the KEEPCARING project, along with the GDPR implementing national legislations.

- This document tracks all the GDPR compliance documentation related to the Project's activities. To facilitate ongoing compliance, Partners must ensure that all data sharing is conducted strictly in line with this document, the Project's policies and the relevant GDPR documentation which will be outlined in the following paragraphs and annexed below in Section 6.
- In addition, this document must be read alongside the DMP, which covers a wider technical scope. As some project activities have already slightly deviated from the initial plan, and in light of the recent changes within the Consortium, the DMP will be updated by the COO every other reporting period.

We have analysed the current status of the Project against the applicable regulatory framework to provide a comprehensive overview of the GDPR obligations. This analysis is categorised into three main areas:

- **Privacy roles:** GDPR defines different roles with different obligations attached. See section 3.1
- **Organisational measures:** GDPR defines a number of organisational and legal measures that must be implemented when processing personal data. These are analysed below in section 3.2 - 3.3.
- **Data subject rights:** See section 3.4.
- **Technical and security controls:** See section 3.5.

For the avoidance of doubt, GDPR remains applicable to all KEEPCARING data processing activities until data are irreversibly anonymised and no longer attributable to any natural person. Anonymisation efficacy must be assessed and documented by each responsible controller.

The following sections detail these requirements and assess the status of the general compliance requirements, suggesting specific actions to mitigate risk. Detailed compliance status reports for specific project activities are provided in Section 4.

3.1 Privacy Roles

3.1.1 Controller

The Controller is the entity that determines the purposes and means of the processing of personal data.

When entities jointly determine the purpose and the means of the processing, they are Joint Controllers and they have to set out the conditions for shared data processing activities, according to art. 26 GDPR:

"*Where two or more controllers jointly determine the purposes and means of processing, they shall be Joint Controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for Data Subjects.*

The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the Joint Controllers vis-à-vis the Data Subjects. The essence of the arrangement shall be made available to the data subject.

Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers".

Requirement 1: Partners contributing to WP2, WP3, WP4, and WP5 may act as either Joint Controllers or Independent Controllers, depending on the specific governance and research setting of each activity. Where Partners jointly determine the purposes and means of processing, they are classified as Joint Controllers and must establish specific Joint Controllership Agreements to regulate their shared responsibilities.

Status
See Section 4 for details about Requirement n.1

3.1.2 Processor and Data Processing Agreements (DPAs)

Where processing is to be carried out on behalf of a controller, the controller must provide specific instructions to the entity acting on its behalf (the processor).

According to art. 28 GDPR "*the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of Data Subjects and the obligations and rights of the controller.*"

A Data processing agreement ("DPA") is an agreement that sets out the conditions for processing personal data between the controller and the processor.

Requirement 2: The Partners relying on other entities to perform the tasks of the Project have to sign a DPA if these entities process personal data on behalf of the Partners.

Status
Each Partner must have a DPA in place with the processors used in the context of the Project

3.1.3 Data Protection Officer (DPO)

In cases defined by article 37 of the GDPR, there is a need to appoint a data protection officer: "*The controller and the processor shall designate a data protection officer in any case where:*

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

- the core activities of the controller or the processor consists of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of Data Subjects on a large scale; or

- the core activities of the controller or the processor consists of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10"

The DPO can be internal or external. However, they must have no existing executive role in the company (e.g. CEO, CTO) in order that they can act independently. The DPO's role is to monitor GDPR compliance, assess data protection risks, advise on data protection impact assessments, and cooperate with regulators and Data Protection Authorities. As such, they need to have real expertise in the area of data protection.

Requirement 3: a DPO should be appointed for the Partners whose processing activities are those indicated in article 37 GDPR.

Status
The Partners which fall under the obligation to appoint a DPO have appointed a DPO

3.1.4 EU Representative

If the organisation has no legal entity within the EU, they must appoint an EU Representative to act as a contact point on their behalf if they offer goods or services to Data Subjects in the EU or if they monitor the behaviour of Data Subjects in the EU.

Requirement 4: The Partners are EU entities. Hogskolen i Innlandet (INN) is a Norwegian entity. All relevant EU data protection instruments, including the GDPR have been implemented by Norway and the other countries of the European Economic Area. An EU Representative is not necessary.

Status
N/A

3.2 Internal documentation

The GDPR poses several obligations on the Controller, in particular internal documentation must be implemented in order to ensure transparency and to demonstrate compliance.

3.2.1 RoPA

Records of processing activities describe full details of what data is collected, under which legal basis it is processed and where the processing happens.

The Record is defined in the GDPR under Art. 30 "*Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:*

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

- the purposes of the processing;

- a description of the categories of Data Subjects and of the categories of personal data;

- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

- where possible, the envisaged time limits for erasure of the different categories of data;

- where possible, a general description of the technical and organisational security measures referred to in Article 32".

Requirement 5: Each Partner acting as a Data Controller must maintain a Record of Processing Activities for the data processing they undertake within the Project. To ensure consistency across the Consortium, the Data Management Plan (DMP) serves as the central reference point.

Action Required: Partners must update their institutional RoPAs to include the Project's activities. When doing so, they must ensure that the definitions of Purposes, Legal Basis, and Data Categories strictly align with those described in the Project's DMP and the relevant Privacy Notices. This ensures that while the records are distributed, the compliance stance remains harmonised.

Status
Distributed Responsibility: Each partner is responsible for updating their local RoPA in alignment with the DMP and Project documentation

3.2.2 Privacy Notices

A privacy notice sets out how and why personal data is being processed and gives details of purposes, legal bases, data subject rights, etc. To be compliant, the privacy notice must reflect the specific processing activities of the corresponding study or data collection activity and needs to ensure that Data Subjects are properly informed about such activities.

Information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. In particular, according to art. 13 of the GDPR, the Privacy Notice addressed to the data subject must cover:

- The name and contact details of the controller
- The contact details of the data protection officer (if appointed)
- The purposes of the processing: why data is collected and used

- The lawful basis for the processing: the legal requirement to process data lawfully[1]
  The legitimate interests for the processing (if applicable)
- The categories of personal data used
- The recipients or categories of recipients of the personal data
- The details of transfers of the personal data to any third countries or international organisations
- The retention periods for the personal data or the criteria used to determine that period
- The rights available to individuals in respect of the processing
- The right to withdraw consent
- The right to lodge a complaint with a supervisory authority
- The source of the personal data (if applicable)
- Details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable)
- Details of any automated decision-making, including profiling (if applicable)

Requirement 6: Data Subjects involved in the different phases of the Project must be informed about the processing activities carried out on their data. A specific privacy notice should be prepared for the different collections which will start according to the tasks of the WPs.
Each Partner directly involved in the collection of data from the Data Subjects must make sure that Data Subjects receive the required information when personal data is collected. They have to make sure that Data Subjects know the name and the contact details of the (joint) controllers and of their data protection officers, the purposes of data processing, the legal basis for processing and be well informed about the data sharing. All this information should be explained in a concise, transparent, intelligible and easily accessible form with clear and simple language at the time of Data Subjects' recruitment for the different tasks of the Project.

[1] These legal bases are indicated in art. 6 of the GDPR and must be relied upon to process common personal data (consent, performance of the contract, compliance with legal obligations, legitimate interest, performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, vital interest). The processing of special categories of data is forbidden by default unless one of the exceptions indicated in art. 9 occurs (among the others, the explicit consent of the Data Subjects, compliance with obligations and exercise of rights in the field of employment and social security, scientific research).

Status
Privacy notices are/will be drafted for all the studies. Notices for upcoming clinical studies (Study A through F) are drafted alongside the study protocols. See Section 4 for further details.

3.2.3 Internal policies and procedures

Internal policies and procedures should be created to govern relevant personal data processing activities. The following policies are the essential ones that must be present in each organisation.

Document	Description
Information Security Privacy Policy	Policy that defines a set of rules and procedures designed to ensure all end users and networks within the organisation meet minimum IT security and data protection security requirements.
Data protection policy (for the personnel)	Policy that defines the general responsibilities and obligations of personnel for the security of personal data. This should include information regarding security controls, relevant data protection requirements and legal obligations.
Data Breach management and Notification Procedure	Policy that describes how the organisation operates in case of a personal Data Breach, pursuant to articles 33 and 34 of GDPR.
Data Breach Register	Register containing records and details of Data Breaches along with mitigation actions performed.

Data Subjects rights enforcement procedure	Policy describing how Data Subjects rights requests should be handled. This should include a list of authorised personnel to handle such requests, the steps to take in order to allow the Data Subjects to exercise their rights and how to effectively enforce them.
Register of Data Subjects Requests	Register containing Data Subjects requests, as well as a brief description of the request and the actions taken in order to fulfil it.
Access control policy	Policy that defines rules and guidelines relating to who has access to given types of data within your organisation.
Asset inventory and asset management policy	Policy that defines the rules to follow in the management of assets (when to use them, who has to use them, security measures applied on, etc.). This should include a detailed asset inventory.
Business Continuity / Disaster Recovery Plan	The set of documented procedures that guide the organisation in how to respond to any outage in such a way that systems can return to a pre-defined level of service. The business continuity plan is for the whole organisation (or its main core business). The disaster recovery plan is related to the IT infrastructure.
Physical and environmental security policy	Policy for the physical security
Backup management policy	Policy for the management of backups
Communications Security Policy	Policy that defines how you ensure the protection of any data transmitted over networks

Requirement 7: Missing policies should be drafted and kept up to date to handle personal data in accordance with the current legislation.

Status
Each Partner adopts its own internal policies and procedures to handle personal data in a GDPR compliant manner

3.3 Risk assessment and DPIA

3.3.1 Risk assessment

A formal risk assessment must be conducted to ensure that the risks posed by any data processing performed have been considered.

In accordance with art. 32 of the GDPR "*Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.*" and "*In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.*"

In some cases, when the risk is high, a Data Protection Impact Assessment ("DPIA") must be performed. Art 35 of the GDPR sets out that "*Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.*

A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

- a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

- processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

- a systematic monitoring of a publicly accessible area on a large scale."

In order to help controllers in identifying when the processing is likely to result in a high risk, the Article 29 Working Party in its Guidelines on Data protection Impact Assessment[2] has provided the following list of characteristics that may be indicative of elevated risk:

- Evaluation or scoring, including profiling and prediction;

- Automated decision making with legal or other significant effects;

- Systematic monitoring;

- Sensitive data on a large scale;

- Data sets that have been matched or combined;

- Data relating to vulnerable subjects;

- Innovative use or application of new technological or organisational solutions;

- Processing that prevents Data Subjects from exercising a right or using a service or a contract.

According to the Impact Assessment Guidelines, a DPIA must be conducted when the processing has two or more of the above characteristics.

Requirement 8: A DPIA must be conducted for some of the activities in Study A, B, C and D. Moreover, a DPIA will be conducted prior to the deployment of the CMP MVP and will be continuously updated as the platform matures.

[2] WP248 https://ec.europa.eu/newsroom/article29/items/611236/en

Status
A DPIA is planned for some of the activities in Study A, B, C and D. Moreover, a DPIA will be conducted prior to the deployment of the CMP MVP and will be continuously updated as the platform matures. For more details see Section 4

3.3.2 3rd country transfer

The GDPR sets out strict rules regarding the transfer of personal data to non-EU countries. Even accessing the data from outside the EU constitutes a data transfer.

Requirement 9: Any data transfers to third countries within the scope of the Project activities must be governed by a valid transfer mechanism as stipulated in the GDPR. These mechanisms are, alternatively, (i) an Adequacy decision for the country in which the data has to be transferred, (ii) the Standard Contractual Clauses ("SCCs") adopted by the EU Commission and signed between the controller and the third party based outside the EU. In this second case, a Transfer Impact Assessment must be conducted to assess if the receiving country offers a protection essentially equivalent to the one offered in the EU.

Status
Every transfer which occurs is covered by either an Adequacy decision or by the SCCs

3.4 Data Subjects Rights

The GDPR grants Data Subjects a number of fundamental rights relating to their personal data.

Right
Right to be informed
Right to withdraw consent
Right of access
Right to rectification

Right to erasure
Right to restrict processing
Right to data portability
Right to object
Rights in relation to automated decision making

3.4.1 Right to be informed

The data controller must ensure that all Data Subjects are informed of the nature and scope of any data processing as well as details of their data subject rights. This obligation is met through the provision of a study-specific Privacy Notice.

Requirement 10: A Privacy Notice must always be available for the Data Subjects. Completed tasks have properly informed Data Subjects about the data processing practices. For the next tasks within the different WPs, Data Subjects will be informed by the Partners collecting the data about the processing activities carried out for the purposes of the Project before the collection starts.

Status
Implemented for T2.2, T2.3 and T2.4 Planned for other tasks before starting the collection

3.4.2 Right to withdraw consent

If data processing depends on consent from the data subject, the controller has an obligation to inform the Data Subjects about their right to withdraw their consent and make the withdrawal possible at any time. Art. 7 of the GDPR sets out that "*the data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.*"

Requirement 11: In the privacy notice(s) Data Subjects are informed about their rights and about the contact details they can use to exercise their right. Should a data subject withdraw the consent, the Partner involved will not use the information collected about the data subject and erase it. This is possible until the data will be aggregated.

Status
Data Subjects can withdraw consent and are/will be informed about it

3.4.3 Right of access

Data Subjects have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;

- the categories of personal data concerned;

- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

- the right to lodge a complaint with a supervisory authority;

- where the personal data are not collected from the data subject, any available information as to their source;

- 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.

Data Subjects can demand a copy of their personal data, provided that their identity is verified through a secure and proportionate method.

Requirements 12: Depending on the processing activities, Data Subjects can access their data by contacting the responsible controller (or Joint Controllers). The primary point of

contact should be the controller (or Joint Controllers) identified in the relevant Privacy Notice. In case of Joint Controllership, all the Joint Controllers have to support each other to provide the information necessary to address the data subject's request. This commitment is set out in the Joint Controllership Agreements.

Status
Data subject can easily access their data by contacting the responsible controller(s)

3.4.4 Right to rectification

If a data subject notifies the controller of any error in their data, this must be corrected without undue delay.

Requirement 13: Information collected by the Partners on the context of the task can be modified, if necessary, by contacting one of the Joint Controllers.

Status
Data Subjects can easily ask for the rectification of data by contacting the responsible controller

3.4.5 Right to erasure

The data subject has a right to ask the controller to delete some or all of their personal data. This must be done immediately, unless there is an overarching reason to continue processing it.

This right is not absolute and the controller must erase the data only when one of the following conditions applies:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

- the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

- the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

- the personal data have been unlawfully processed;

- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

- the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

Requirement 14: If Data Subjects withdraw their consent, the Joint Controllers must erase the personal data. If Data Subjects ask one of the Joint Controllers to erase their data, it means that they withdraw their consent and the Joint Controllers have to erase the personal data.

In any case, the Joint Controllers will have to erase personal identifying information after the time indicated in the privacy notice as the data retention period.

Status
Data Subjects can ask for the erasure of data by contacting one of the Joint Controllers. Personal identifying information will be deleted when the data retention period is completed

3.4.6 Right to restrict processing

A data subject can ask the controller to restrict the processing of their data where one of the following applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

- the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

Requirement 15: A technical solution to quarantine the data in case the data subject exercises the right of restriction should be implemented by the Partners.

Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.

The CMP will implement a solution to restrict the processing of data.

Status
Each Partner collecting personal identifying information has implemented its own technical solution to address the restriction's requests. Planned for the CMP

3.4.7 Right to data portability

The Data Subjects have the right to receive the personal data concerning them, which they have provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

- the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

- the processing is carried out by automated means.

Requirement 16: When the processing relies on consent or on the contract and is carried out by automated means, each joint controller involved in the processing of data under a specific task must be ready to provide a copy of the data in a structured, commonly used and machine-readable format (PDF, JSON, CSV, etc.)

In the CMP users should be able to download the data pertaining to them.

Status
Each Partner involved in a processing of personal data based on consent or on the contract and using automated means can provide a copy of the data from their system. The CMP will provide a copy of the users' data by accessing the user's profile.

3.4.8 Right to object

The data subject has a right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (point (e) of art. 6.1) or based on the legitimate interest of the controller or of a third party (point f) of art. 6.1), including profiling based on those provisions.

Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1) GDPR, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data

concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

The controller must no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Requirement 17: If the legal basis of the processing used by the Partners for the processing of data under a specific task is the legitimate interest or the performance of a task carried out in the public interest, the right can be exercised by the Data Subjects.

In addition, some data may be processed to ensure the security of the CMP (usage data of the users) and this processing could be based on the legitimate interest of the controller(s). Therefore, the right to object should be mentioned in the privacy policy that will be provided to the platform users.

The Data Subjects must be able to contact the controller(s) to exercise their right to object.

Status
Data Subjects can object to the processing of their personal data when the conditions of art. 21 GDPR are met by contacting one of the controllers

3.4.9 Rights in relation to automated decision making

Art. 22 of the GDPR sets out that

"*The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.*

Paragraph 1 shall not apply if the decision:

a) *is necessary for entering into, or performance of, a contract between the data subject and a data controller;*
b) *is authorised by Union or Member State law to which the controller is subject, and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or*

c) is based on the data subject's explicit consent.

In the cases referred to in points a) and c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place."

Requirements 18: Currently, art. 22 is not applicable to the processing carried out in the context of the Project. No decision will be taken based on the processing activities carried out within the project.

Status
N/A

3.5 Technical and Security Control

To effectively manage the diverse data processing activities within KEEPCARING, the Consortium has adopted a dual-layer approach to technical security. This distinction is necessary to address the operational differences between the established clinical environments and the innovative digital tools under development.

- **Layer 1: Distributed Research Environment (Current Status):** The majority of data processing currently undertaken (e.g., clinical studies A through F) occurs within the infrastructures of the beneficiary institutions (Universities and Hospitals). Consequently, technical security is governed by the stringent institutional policies and IT standards of these organisations. These environments are subject to rigorous internal oversight, ensuring that data storage and handling meet high-level security requirements without the need for additional project-level intervention at this stage.
- **Layer 2: Centralized Platform Environment (Future Implementation):** The second layer concerns the KEEPCARING Change Management Platform (CMP). The security validation strategy for this component has been specifically adapted to manage the

transition of the technical lead from NURO to DIGITALTWIN. To ensure the security audit is legally valid, the Consortium determined that the formal assessment and Data Protection Impact Assessment (DPIA) must be executed on the updated DIGITALTWIN infrastructure. This ensures that the compliance assessment applies to the active production environment that will process end-user data.

Mitigation Plan: A comprehensive security assessment and a specific Data Protection Impact Assessment (DPIA) are scheduled to take place as the platform matures. This ensures that the security validation is performed on the current architecture, thereby providing a true reflection of the platform's compliance posture, while aligning with the General Assembly decisions on key topics regarding the CMP development.

4. Data processing activities carried out within the Project

The Project's activities are structured along two primary lines: research activities (encompassing WP2, WP3, WP4, and WP5) and technical development, which includes the website and the foundational work for the Change Management Platform (CMP) under WP5, such as the initial co-design events.

From a GDPR perspective, these distinct work streams entail different requirements. Consequently, the compliance framework has been tailored to address the specific needs of each individual activity. Comprehensive details regarding the data processing activities are available in the Project's Data Management Plan (DMP) and the annexed documentation to the present document. Broadly, the Project involves the processing of both general personal data (e.g., email addresses, demographics, professional experience) and special categories of personal data as defined under the GDPR, such as health data.

The following sections provide a description of each project activity and its associated compliance details.

For research activities, the information provided below should be read in conjunction with the research protocols of each individual study.

Furthermore, specific protocols are in place regarding data publication and quality assurance to make anonymized project data publicly available. The project adheres to the "KEEPCARING guideline for data management and collection" to standardize these

procedures. Prior to sharing any dataset via Zenodo, a mandatory quality check is performed using a pre-determined procedure to rigorously verify anonymization. As outlined in the DMP, anonymized datasets collected in Castor or Qualtrics will be archived in Zenodo by the respective Work Package leaders at the end of the project. Please note that both the KEEPCARING guideline and the DMP are living documents, periodically updated to fully reflect project developments.

4.1 Study A - Resilience factors an observational cross-sectional study in healthcare workers

The study objectives: The study aims to assess and predict levels of resilience and burnout among hospital-based nursing and medical personnel and how do factors like work setting factors influence them. This information will help to understand how burnout happens, what factors make it happen, and what the health services can do about it.

Study A is being conducted in different phases, following the Work Package 2 structure. In particular, four main different phases are identified:

1) **Online surveys (T2.3)**
    - **Controllers**: UL, RIGS, UKE, AUMC, NOVA under the Joint Controllership Agreement for WP2 - Study A activities.
    - **Lead Researchers:** Stephen Gallagher (Stephen.Gallagher@ul.ie) and Trina Tamrakar (Trina.Tamrakar@ul.ie) from UL.
    - **Status**: Survey administration has been completed. An assessment of the anonymisation process is planned prior to the sharing of the dataset.
    - **Purpose**: This phase of the study aims to examine, via a survey, levels of burnout among hospital-based nursing and medical personnel in several EU countries (starting with Ireland, Denmark, Germany and Netherlands) and to explore the determinants of this from an individual, social, management and systems level. Data processing activities are conducted to achieve these purposes.
    - **Data Subjects:** Health care professionals (in hospital settings).
    - **Special categories of personal data:** Ethnicity data and health related data.

- **Legal basis for the processing and exception required to process special categories of** data: Public interest (art. 6(1)(e)) and Scientific Research (art. 9(2)(j)).
- **DPIA**: Taking into account the nature (online survey; not a new technology), the scope (examine burn out levels to contribute to the research project with the aim of combatting such phenomena), context (an external University collecting data from collaborating hospitals, in different states) and purposes (see above) of the processing activities, no high risk to the rights and freedoms of natural persons were identified. Furthermore, despite the relatively high number of participants, the large-scale requirement was not met given the total population of the staff employed in the participating hospitals.
- **Data sharing/Recipients:** This phase of Study A utilised Qualtrics as the primary tool for structuring and administering the survey. The resulting dataset will be uploaded to UL's SharePoint to facilitate access for the Data Controllers.
- **Data retention:** Email addresses are stored for 36 months starting from the end of the survey. All research data will be kept for 7 years from the end of the survey.
- **Privacy Notice:** Provided to the participants. See annex 1.1.
- **Notes:** A Joint Controllership Agreement was drafted by UL legal offices and it's now in the final stages of the signing process. This regulates the obligations of the controllers and the data sharing between them as per the Project plan.
  Regarding the ethnicity data collected, a specific review to ensure compliance with the national regulations of recipient Partners will be conducted, with particular attention to potential restrictions or prohibitions.

  For the updated WP2 JCA text, please refer to Annex 2.1.

2) **Follow up qualitative interviews (T2.2)**
   - **Controller**: UL, autonomous Data Controller.
   - **Lead Researchers:** Stephen Gallagher (Stephen.Gallagher@ul.ie) and Trina Tamrakar (Trina.Tamrakar@ul.ie).
   - **Status**: Ongoing, last interviews to be conducted by Q4 2025/Q1 2026.
   - **Purpose**: This phase of the study aims to gather the views and experiences of healthcare professionals regarding burnout in the four participating countries

through one-on-one interviews. Data processing activities are conducted to achieve this purpose.

- **Data Subjects:** Health care professionals (in hospital).
- **Special categories of personal data:** Health related data.
- **Legal basis for the processing and exception required to process special categories of data:** Consent (art. 6(1)(a) GDPR) and explicit consent (art. 9(2)(a) GDPR).
- **DPIA**: Taking into account the nature (1-to-1 interviews; not a new technology), the scope (examine burn out levels to contribute to the research project with the aim of combatting such phenomena), context (an external University collecting data from collaborating hospitals, in different states) and purposes (see above) of the processing activities, no high risk to the rights and freedoms of natural persons were identified. Furthermore, the small number of participants and the fact that only UL will have access to the data collected from the interviews, strengthen the conclusion reached.
- **Data sharing/Recipients:** This phase of Study A used Qualtrics as the main tool for administering the enrolment process, while it used UL Microsoft Teams to conduct the interviews.
- **Data retention:** All research data will be kept for 7 years from the end of the survey.
- **Privacy Notice:** Provided to the participants. See Annex 1.1.2.
- **Notes:** Unlike Phase 1, the data collected in these interviews will not be shared among Project Partners and will be analysed exclusively by UL.

3) **Hexoskin pilot (T2.4)**
   - **Controller(s)**: UL, RIGS, UKE, AUMC, NOVA under the Joint Controllership Agreement for WP2 - Study A activities.
   - **Lead Researchers:** Laetitia Zoe Hampe (l.hampe@uke.de) from UKE and Luis Silva (lmd.silva@fct.unl.pt) from NOVA.
   - **Status**: Staff counsel approved the pilot only after receiving strong guarantees regarding the access to the data. In this sense, only the Lead Researchers will have access to the data collected from the Hexoskin, excluding any possibility for staff with HR functions to access employee's data.
   - **Purpose**: The aim of this pilot study is to evaluate the feasibility of measuring stress and resilience in healthcare workers during daily clinical activity on the ward using Hexoskin. The results serve as a basis for a subsequent study in which bio-psycho-social risk and protective factors are to be identified and verified in order to finally develop bio-behavioural models for predicting

resilience. Data processing activities are conducted to achieve these purposes.

- **Data Subjects:** Health care professionals (in hospital).
- **Special categories of personal data:** Health related data.
- **Legal basis for the processing and exception required to process special categories of data**: Consent (art. 6(1)(a) GDPR) and explicit consent art. 9(2)(a) GDPR.
- **DPIA**: A DPIA was deemed necessary since the study meets at least three of the criteria set out by the WP29 Guidelines. Specifically, the Study will involve vulnerable subjects (employees of the healthcare institution), even if in a limited number (4 employees), it will process special categories of personal data (physiological and health data collected via the Hexoskin wearable technology) and it will involve the use of a new technology, at least given the specific context of monitoring stress markers in a workplace setting. We expect the DPIA to be ready in Q1 2026, before the starting date of the processing activities.
- **Data sharing/Recipients:** This phase of Study A uses Hexoskin and their cloud technology to collect and store the data. Data transfer to Hexoskin will be strictly regulated. Regarding the cloud storage provider used by Hexoskin, the applicability of the German BSI C5 certification (Cloud Computing Compliance Criteria Catalogue) is currently being assessed, considering that C5 certification is typically a mandatory regulatory requirement for the processing of patient data within German hospital infrastructures.
  The questionnaire part of this phase will be managed on Castor, and the data will be further stored in Zenodo.
- **Data retention:** To be defined.
- **Privacy Notice:** See Annex 1.1.3.
- **Notes:** A Joint Controllership Agreement was drafted by UL legal offices and it's now in the final stages of the signing process. Only UKE and NOVA will access the survey data and Hexoskin data to tackle the related tasks under WP2 and WP5, while the other Partners involved will only be informed about anonymous aggregated results. For the updated WP2 JCA text, see Annex 2.1.

4) **Hexoskin study** (T2.4 - DPIA needed)
   - **Controller(s):** UKE and NOVA, Joint Controllers.
   - **Lead Researchers:** UKE
   - **Status:** The study protocol is under development. The Consortium is currently organising the strategy for the ethical approval process.

- **Purpose:** To be refined. The study protocol for this final phase is currently under development.
- **Data Subjects:** Health care professionals.
- **Special categories of personal data:** Health-related data.
- **Legal basis for the processing and exception required to process special categories of data:** Consent (art. 6(1)(a) GDPR) and explicit consent art. 9(2)(a) GDPR.
- **DPIA:** A DPIA was deemed necessary since the study meets at least three of the criteria set out by the WP29 Guidelines. Specifically, the Study will involve vulnerable subjects (employees of the healthcare institution), it will process special categories of personal data (physiological and health data collected via the Hexoskin wearable technology) and it will involve the use of a new technology, at least given the specific context of monitoring stress markers in a workplace setting. We expect the DPIA to be ready in Q2 2026, before the starting date of the processing activities.
- **Data sharing/Recipients:** Access to data will be limited to the strictest extent possible. This phase of Study A uses Hexoskin and their cloud technology to collect and store the data. Data is transferred to Hexosking only in the presence of the safeguards mandated by the GDPR. Regarding the cloud storage provider used by Hexoskin, the applicability of the German BSI C5 certification (Cloud Computing Compliance Criteria Catalogue) is currently being assessed, considering that C5 certification is typically a mandatory regulatory requirement for the processing of patient data within German hospital infrastructures.
  The questionnaire part of this phase will be managed on Castor, and the data will be further stored in Zenodo.
- **Data retention:** To be defined.
- **Privacy Notice:** To be drafted.
- **Notes:** Following an internal reorganization of the tasks in WP2, this study will take place exclusively at UKE. A specific Joint Controllership Agreement (JCA) will consequently be drafted to regulate the relationship between UKE and NOVA for this specific phase.

4.2 Study B - Deep relaxation using Virtual Reality intervention before surgery for healthcare professionals working in the operating room

The study objectives: The goal of this research is to better understand if, and to what extent, a Virtual Reality (VR) intervention can help to reduce stress in the workplace. It will look at how people experience their stress (via questionnaires) before and after the intervention, but also at physical signals of stress, such as heart rate and heart rate variability. There will be a comparison between the effects of the VR headset with those of a quiet (low stimulus) environment. Additionally, it will be investigated how satisfied participants are with both interventions and how cost-effective the interventions are.

- **Controller (s):** AUMC RIGS and UKE, which are going to sign a Joint Controllership agreement for the execution of this Study.
- **Lead Researchers:** Sophie Vermeulen from AUMC (s.q.vermeulen@amsterdamumc.nl).
- **Status**: Ethical approval obtained in AUMC. UKE and RIGS will follow. Start of the study expected in Q1 2026.
- **Purpose**: Data processing activities are carried out to achieve the Study objectives.
- **Data Subjects:** Health care professionals.
- **Special categories of personal data:** Health related data.
- **Legal basis for the processing and exception required to process special categories of data**: Consent (art. 6(1)(a) GDPR) and explicit consent (art. 9(2)(a) GDPR).
- **DPIA**: A DPIA was deemed necessary since the study meets at least three of the criteria set out by the WP29 Guidelines. Specifically, the Study will involve vulnerable subjects (employees), it will process special categories of personal data (health data such as heart rate, heart rate variability) and it will involve the use of a new technology, at least given the specific context in which the technology is used. We expect the DPIA to be ready in December 2025, January 2026 at the latest, before the starting date of the processing activities.
- **Data sharing/Recipients:** Data will be collected on the researcher's laptop and later uploaded to Castor as the main data repository. Data won't be shared outside the Joint Controllers. Only aggregated anonymous data will be used in scientific publications.
  Furthermore, it has been clarified that Healthy Mind—the provider of the VR headsets and simulation software—will not be designated as a Data Processor. This

determination is based on the fact that Healthy Mind will not have access to any personal data collected within the context of the Study.

- **Data retention:** 5 years after study completion.
- **Privacy Notice:** PN ready to be added to the informed consent module (the latter not modifiable under AUMC policies). See annex 1.2.
- **Notes:** A Joint Controllership Agreement was drafted, approved by AUMC legal office, and it's now under review in UKE and RIGS. This will regulate the joint research activities. See annex 2.3 for the version currently under review in UKE and RIGS.
  To address the potential imbalance of power inherent in consent collection within an employment context, specific mitigation strategies are currently under evaluation. Regarding AUMC, the engagement of an external entity acting as a data processor is being defined to manage consent collection. For the other participating hospitals, the specific approach is currently under review. Following discussions with local legal and ethics offices, a potential solution is the cross-collection of data to decouple the research activity from the direct employer–employee relationship. This approach will be aligned with the mitigation strategy adopted in Study B, ensuring that the research activities are clearly separated from the employment relationship. Furthermore, robust pseudonymisation measures will be implemented as stipulated in the Joint Controllership Agreement (JCA). The precise operational steps for these measures are being finalised in collaboration with the Lead Researcher and will be comprehensively documented in the forthcoming DPIA.

4.3 Study C - Evaluating Healthcare Professionals' Satisfaction and Stress Mitigation Using Virtual Reality Intervention in Surgical Ward: a multination feasibility study

The study objectives: The main goal of this research is to gain insight into the feasibility, acceptance, and satisfaction of healthcare professionals on surgical wards regarding a Virtual Reality (VR) intervention.
Researchers are looking at user comfort and studying how VR can best be integrated into daily practice. Additionally, we are investigating the effect of the intervention on the perceived stress level before and after using VR.

- **Controller (s) Responsible Partner**: AUMC. Joint Data controller along with RIGS and UKE, which are going to sign a Joint Controllership agreement for the execution of this Study

- **Lead Researchers:** Sophie Vermeulen (s.q.vermeulen@amsterdamumc.nl) and Anne Eskes (a.m.eskes@amsterdamumc.nl) from AUMC.
- **Status**: Ethical approval underway in AUMC. UKE and RIGS will follow. Start of the study expected in Q1 2026.
- **Purpose**: Data processing activities are carried out to achieve strictly connected with the Study objectives.
- **Data Subjects:** Health care professionals.
- **Special categories of personal data:** health related data. Physiological data (heart rate and heart rate variability) will be measured in real-time during the trial session but will not be recorded or stored for subsequent analysis.
- **Legal basis for the processing and exception required to process special categories of data:** Consent (art. 6(1)(a) GDPR) and explicit consent (art. 9(2)(a) GDPR).
- **DPIA:** The DPIA for Study B will cover Study C activities as well, with a specific section focusing on the latter.
- **Data sharing/Recipients:** Data will be collected on the researcher's laptop and later uploaded to Castor as the main data repository. Data won't be shared outside the Joint Controllers. Only aggregated anonymous data will be used in scientific publications.
  Furthermore, it has been clarified that Healthy Mind - the provider of the VR headsets and simulation software - will not be designated as a Data Processor. This determination is based on the fact that Healthy Mind will not have access to any personal data collected within the context of the Study.
- **Data retention:** 5 years after study completion.
- **Privacy Notice:** A Privacy Notice has been drafted and is ready to be integrated into the informed consent module (noting that the module structure is not modifiable under AUMC policies). See Annex 1.3.
- **Notes:** A Joint Controllership Agreement was drafted and is currently in the final stages of the review process. This will regulate the joint research activities. Please refer to Annex 2.3 for the version currently under review by UKE and RIGS.

Regarding the collection of consent within the employment context, a different approach is adopted here compared to Study B. For this specific feasibility study at AUMC, reliance on an external recruitment site to mitigate power imbalance risks was not deemed necessary. This decision is justified by the limited scope of the study and the fact that sensitive physiological data is immediately discarded after measurement, thereby significantly reducing the risk profile.

For the remaining participating Partners (UKE and RIGS), an assessment is currently underway to determine if this simplified approach satisfies their local institutional requirements or if additional safeguards are required. In all cases, robust pseudonymisation measures will be strictly enforced.

4.4 Study D - Study D - Longer term resilience Team debriefing after surgery

The study objectives: The objective of this study is to evaluate the impact of structured postoperative debriefings with and without procedural, structured audio- and video recordings, on team performance, psychological safety, and non-technical skills in the operating room. Specifically, this study aims to compare augmented debriefings with non-augmented debriefings, to assess differences in perceived usefulness, psychological safety, and observed improvements in teams' non-technical skills.

- **Controller(s)**: RIGS, AUMC and UKE.
- **Lead Researchers:** Jeanett Strandbygaard (jeanett.strandbygaard@regionh.dk) and Johanne Soeborg Hartmann (johanne.soeborg.hartmann@regionh.dk) from RIGS.
- **Status**: The ORBB system has been in use in RIGS - after local and national legal approval - for two years. RIGS' ethics committee has already approved the research protocol for this specific study, and the informed consent module and privacy notice have been drafted. Data collection for the purpose of the study will start once the DPIA has been completed.
  AUMC is in the process of installing and approving the ORBB system in their premises. Both AUMC and UKE will need to obtain ethics approval before starting the data collection activities.
- **Purpose**: Data processing activities are carried out to achieve the Study objectives.
- **Data Subjects:** Health care professionals; Patients undergoing surgery.
- **Special categories of personal data:** Patient's health data (laparoscope data).
- **Legal basis for the processing and exception required to process special categories of data**: Consent (art. 6(1)(a) GDPR) and explicit consent (art. 9(2)(a) GDPR, for patients).
- **DPIA**: Taking into account the nature (cameras and microphones system monitoring the OR), the scope (assessing team performance, psychological safety, and non-technical skills in the operating room through an ORBB-augmented and non-augmented setting), context (Hospitals analysing data coming from their employees) and purposes (see above) of the processing activities, a DPIA was

deemed necessary since the study meets at least two of the criteria set out by the WP29 Guidelines. Specifically, the Study will involve vulnerable subjects (employees), and it will involve the use of a new technology, at least given the specific context in which the technology is used. We expect the DPIA to be ready in December 2025, January 2026 at the latest, before the starting date of the processing activities.

- **Data sharing/Recipients:** Castor will be used as the main data repository, along with Zenodo for long term storage. Surgical Safety Technologies, Inc. (Toronto, Canada; "SST"), provider of the ORBB system, will have access to the audio-visual data produced by the ORBB and uploaded to their cloud storage and to patient data processed in the same context. Data is transferred to SST only in the presence of the safeguards mandated by the GDPR.
- **Data retention:** 15 years after project completion.
- **Privacy Notice:** See annex 1.4 (for health care professionals).
- **Notes:** A Joint Controllership Agreement was drafted, approved by AUMC legal office, and it's now under review in UKE and RIGS. This will regulate the joint research activities. See annex 2.3 for the version currently under review in UKE and RIGS.
  Specific mitigation strategies are currently under evaluation to address the potential imbalance of power inherent in consent collection within an employment context. The specific approach is currently under review, following discussion with local legal and ethics offices. Furthermore, robust pseudonymisation measures will be implemented as stipulated in the Joint Controllership Agreement (JCA), and in line with the security measures implemented by default by SST.
  Finally, patients consent collection flows and information will follow the Hospitals' internal policies, in line with applicable laws.

4.5 Study E - Co-work design: A structural approach to reduce individual work stress in healthcare professionals in hospital settings

The Study objectives: The goal of this study is to learn, through a questionnaire, what nursing professionals' work looks like and to what extent they can redesign their work environment together with their colleagues (this is called co-work design) to reduce work stress and improve their well-being.

  - **Controller(s)**: EUR, Autonomous Data controller. Participating hospitals, Autonomous Data controller.

- **Lead Researchers:** Luisa Solms (solms@essb.eur.nl).
- **Status**: Ongoing. Data collection started in AUMC and RIGS following the GDPR framework for Study E (see Annex 2.4).
- **Purpose**: Data processing activities are conducted to pursue the study objective.
- **Data Subjects:** Health care professionals.
- **Special categories of personal data:** Health related data.
- **Legal basis for the processing and exception required to process special categories of data**: Consent (art. 6(1)(a) GDPR) and explicit consent art. 9(2)(a) GDPR.
- **DPIA**: Taking into account the nature (online survey; not a new technology), the scope (analyse pro-social job crafting predisposition and potentiality), context (an external University collecting data from collaborating hospitals, in different states) and purposes (see above) of the processing activities, no high risk to the rights and freedoms of natural persons were identified. Furthermore, despite the relatively high number of participants, the large-scale requirement is not met given the total population of the staff employed in the participating hospitals.
- **Data sharing/Recipients:** This Study uses Qualtrics as the main tool for structuring and administering the survey. Contact data is collected in AUMC, RIGS and other participating sites and with the consent of the participants is shared with EUR for the purpose of administering the surveys constituting this Study. With the consent of the participants, only pseudonymised data will be shared with Participating Hospitals when these want to access individual-level data. Otherwise, only aggregated data will be shared.
- **Data retention:** 10 years after Study completion.
- **Privacy Notice:** See annex 1.5, 1.5.2, 1.5.3.
- **Notes:** An ad hoc GDPR framework has been developed to provide guidelines for this specific Study and to explain the data sharing between the involved Partners. The framework is annexed below in section six as Annex 2.4, along with the related template privacy notices.

4.6 Study F - Study F WP5 - Mitigating toxic leadership styles through the development of a compassionate motivation in the workforce of healthcare workplace

The Study Objective in a nutshell: This project aims to develop and evaluate the impact of an 8-sessions online psychological intervention designed to help healthcare professionals working in Portuguese hospitals (in both leadership and non-leadership roles).

- **Controller(s)**: UC. Data Controller.
- **Lead Researchers:** Diana dos Santos Ribeiro da Silva (diana.rs@fpce.uc.pt).
- **Participating Partners:** DIGITALTWIN. Role has not been defined yet.
- **Status**: Ethical approval obtained in UoC. Start of the study expected in Q1 2027.
- **Purpose**: Data processing activities are conducted to achieve the Study objectives.
- **Data Subjects:** Health care professionals.
- **Special categories of personal data:** Health related data.
- **Legal basis for the processing and exception required to process special categories of data**: Consent (art. 6(1)(a) GDPR) and explicit consent art. 9(2)(a) GDPR will be likely used in study F as well.
- **DPIA**: The necessity of conducting a specific Study DPIA will be assessed once the intervention structure is clearer in terms, in particular, of technologies involved.
- **Data sharing/Recipients:** The Study will rely on the KEEPCARING CMP to integrate the iWORK.COMP program. However, specific technical workflows are still being defined, particularly regarding the interaction between the project website, the CMP, and external providers used for administration. It is anticipated that data collection tools (e.g. Qualtrics) could be used.
- **Data retention:** 5 years after study completion.
- **Privacy Notice:** PN will be produced.
- **Notes:** The GDPR roles in this Study will be assessed, focusing on the role of DIGITALTWIN as a research participant (Data processor or Joint controller) once the platform development (see section 4.8) will be in a more advanced status.

4.7 The Website

Initial compliance for the KEECPARING webpage was successfully completed. The roles related to the processing activities carried out through the website have been defined and a JCA has been signed, the privacy notice and the cookie policy have been adopted. However, due to a recent change in the technical Partners from NURO to DIGITALTWIN, these documents require a revision. In particular, DIGITALTWIN and CONNECTOR will need to sign a new JCA.

JCA	Annex 2.6
PN	Annex 2.6
Cookie Policy	Annex 1.7

4.8 The KEEPCARING Change Management Platform (CMP)

The KEEPCARING Change Management Platform (CMP) represents the central digital output of the project, developed under Work Package 5.

From a data protection perspective, the design and development of the CMP involve two distinct streams of data processing, each with specific requirements:

- **Co-design Activities (Section 4.8.1):** The participatory research phase where end-users (healthcare professionals) contribute to the design of the solution.
- **Platform Development & Compliance (Section 4.8.2):** The technical implementation of the platform, specifically regarding the transition of technical Partners (from NURO to DIGITALTWIN), the definition of data flows from the clinical studies, and the training of the underlying AI models.

The following sections detail the compliance status and risk mitigation strategies for these respective phases.

4.8.1 Co-design activities

The activity objectives: The co-design event is the first step towards the creation of the KEEPCARING Change Management Platform (CMP), part of the project's solution package. The CMP will be a companion app for mobile devices presenting goals and mission, overview, innovative integrative solutions (active interaction with end-users, participative scenarios, assessment forms) and management approaches able to impact organizational models to support healthcare decision-makers in addressing stress and burnout among healthcare professionals.

- **Controller(s)**: CNR. Data Controller
- **Lead Researchers:** Maria Chiara Caschera (mariachiara.caschera@cnr.it).
- **Purpose**: Collect co-design feedback from potential future users of the CMP.
- **Status**: First event completed.
- **Special categories of personal data: None.**
- **Legal basis for the processing**: Consent (art. 6(1)(a) GDPR).
- **DPIA**: N/A.
- **Data sharing/Recipients:** The data is collected through the researcher's laptop. After anonymization and aggregation, it is uploaded on the project's Microsoft One drive.
- **Data retention:** Name and contact details will be deleted within 1 year after completion of the research.
- **Privacy Notice:** See annex 1.8.
- **Notes:** No Study protocol and Ethical approval was needed for this co-design activity. However, the participants were properly informed about the details of their participation, and photos and videos were taken during the event, in line with GDPR requirements (see Annex 1.8).
  Names and contact information of the participants were not associated with the data collected through the audio/video recording, the "Slido" tool and the conclusive questionnaire.

4.8.2 CMP development and compliance work

Following the succession in the technical leadership role from NURO to DIGITALTWIN, DIGITALTWIN has developed an updated version of the initial Minimum Viable Product (MVP) of the Change Management Platform (CMP). Access to a demo account was provided on 20 November 2025.

The compliance status of the updated CMP will continue to be assessed and the necessary legal documentation will be integrated. Specifically, the following compliance deliverables will be produced:

- **Privacy Notices:** Tailored to the distinct categories of Data Subjects that will use the platform (to be defined).
- **Cookie Policy:** To ensure compliance with the ePrivacy Directive.
- **Joint Controllership Agreement (JCA):** To be drafted if deemed necessary following an assessment of the shared purposes, the platform's ownership and controllership structure.
- **DPIA / Risk Assessment:** This will be finalised by Month 24, in the form of Milestone 7 of the Project.

Integration of AI Models and Data Flows (Relation to Deliverable 5.3) A critical aspect of the CMP's future development involves the integration of AI models currently under discussion with NOVA. Preliminary assessments identify two main components for AI training:

1. A model based on psychometric data (demographic data and questionnaires answers).
2. A model based on physiological data (e.g., Heart Rate Variability, Hexoskin data).

Regarding the privacy implications of this training, it is established that development will be conducted on individual level de-identified data. Furthermore, safeguards will be implemented to ensure that once training is complete, the resulting model will not permit the singling out of natural persons.

In alignment with the AI Act, specific obligations regarding transparency, human oversight, and auditability will be enforced. To ensure traceability and compliance, the system design will require the maintenance of audit logs, model update records, and comprehensive dataset documentation.

Strategic Next Steps

To establish a solid foundation for these advancements, CHINO will initiate a legal roadmap that will serve as the legal backbone for the CMP development. This roadmap will explicitly outline which CMP functionalities may legally be implemented and the required sequence of implementation to ensure full alignment with GDPR, MDR, and the AI Act and applicable legislation.

The specific technical methodologies - including the type of models selected and the training protocols - will be comprehensively documented in **Deliverable 5.3**. Consequently, the GDPR Framework will require subsequent updates to address how these models are integrated into the CMP architecture.

A priority for upcoming General Assemblies is to define the precise data flows between the clinical studies and the CMP. Specifically, the Consortium must determine exactly which data subsets from the project activities will be transferred to or used within the platform. This assessment is essential to ensure that the final technical architecture remains fully aligned with the Project's privacy obligations.

Crucially, it must be noted that, at this stage, Data Subjects participating in the clinical studies have not been explicitly informed regarding the direct usage of their personal data within the CMP environment. Consequently, specific transparency and information activities - such as the issuance of supplementary Privacy Notices or consent addenda - might be required prior to any data ingestion into the platform.

Furthermore, regarding the definition of user roles within the platform (currently distinguished between "Organisations" and "Individual Healthcare Professionals"), strict access controls must be enforced. Specifically, access to individual-level data must be rigorously excluded for anyone but the individual, with organisational roles (e.g., HR Managers or Hospital Managers) allowed to access only aggregated data, provided this aligns with applicable national legislation. This restriction is mandated by the sensitivities inherent in the employment context: it is essential to ensure that the platform serves as a tool for support rather than a mechanism for employee monitoring or individual performance evaluation.

Technical Security Implementation In accordance with the dual-layer strategy defined in Section 3.1, the operational security assessment has been synchronized with the technical handover. With DIGITALTWIN having released the updated Minimum Viable Product (MVP) in November 2025, the compliance work has moved from the transition phase to the validation phase. Consequently, the security controls and the platform-specific DPIA will be executed against this consolidated architecture, ensuring that all protective measures are verified prior to the ingestion of any clinical data.

5. Summary tables

This section presents summary tables mapping the compliance documents detailed in Section 4 to their corresponding Annexes in Section 6.
Documents not marked as "final" will be subject to revision as the project evolves. Furthermore, documentation for activities currently listed as "planned" will be drafted and finalized as those specific tasks approach implementation. These updates will be uploaded to the Project SharePoint and formally annexed in the future update of Deliverable 7.1 or in Deliverable 7.2.

Table 5.1 - Privacy Notices

	Annex n.	Status	Responsible partner(s)
Study A - Phase 1	1.1	Completed and final	UL
Study A - Phase 2	1.1.2	Completed and final	UL
Study A - Phase 3	1.1.3	Draft ready, to be reviewed	UKE, NOVA
Study A - Phase 4	1.1.4	Planned	UKE, NOVA
Study B	1.2	Draft ready, to be reviewed	AUMC, RIGS, UKE
Study C	1.3	Draft ready, to be reviewed	AUMC, RIGS, UKE
Study D	1.4	Draft ready, to be reviewed	AUMC, RIGS, UKE
Study E - Privacy Notice EUR - study administration	1.5	Completed and final	EUR
Study E - Privacy	1.5.2	Completed and final	EUR

Notice participating hospitals - no data analysis			
Study E - Privacy Notice participating hospitals - with data analysis	1.5.3	Completed and final	EUR
Study F	1.6	Planned	UoC
Website	1.7 (cookie policy). See also 2.6	Completed and final. NURO → DTT to be addressed	AUMC, DTT
CMP Co-design event	1.8	Completed and final	CNR
CMP	1.9	Planned	DTT

Table 5.2 - Joint Controllership Agreement

	Annex n.	**Status**	**Responsible partner(s)**
Study A - Phases 1, 2 and 3	2.1	Signature process ongoing	UL, NOVA, UoC, UKE, RIGS
Study A - Phase 4	2.2	Planned	UKE, NOVA
Study B, C and D	2.3	Review ongoing in UKE and RIGS	AUMC, UKE, RIGS
Study E	2.4, GDPR framework	Not a JCA - see annex	EUR

Study F	2.5	Planned (if necessary)	UoC
Website	2.6	Completed. NURO → DTT to be addressed	AUMC, DTT
CMP	2.7	Planned (if necessary)	DTT

Table 5.3 - Data Protection Impact Assessment (DPIA)

	Annex n.	**Status**	**Responsible partner(s)**
Study A - Step 4	N/A	Planned for Q2/Q3 2026	UKE, NOVA
Study B	N/A	Planned for Q1 2026	AUMC, RIGS, UKE
Study C	N/A	Planned for Q1 2026	AUMC, RIGS, UKE
Study D	N/A	Planned for Q1 2026	AUMC, RIGS, UKE
Study E	N/A	N/A	N/A
Study F	N/A	Planned for Q4 2026	UoC
Website	N/A	N/A	N/A
CMP - Codesign event	N/A	Planned for Q2 2026	DTT

Table 5.4 - Action Plan

CHINO will collaborate with the designated Partners to draft the documentation outlined below. The following table establishes the roadmap for 2026 and projects key compliance

activities through to the project's conclusion. Where applicable, requirement reference numbers from Section 3 are included for traceability.

Interested project activity	Requirement	Status	Responsible partner(s)	Due date
Study A – Phase 3	N.2 - DPA - Relationship with Hexoskin	To be assessed, including C5 certification applicability	UKE, NOVA	Q1 2026
Study A – Phase 3	N.9 - International data transfers - Relationship with Hexoskin	Transfer Impact Assessment (TIA) to be drafted; SCC to be drafted and signed	UKE, NOVA	Q1 2026
Study A – Phase 3	N.6 - Privacy Notice	Draft ready, to be reviewed by UKE	UKE	Q1 2026
Study A – Phase 3	N.8 - DPIA	Planned	UKE, NOVA	Q1 2026

Study A – Phase 4	N.1 - JCA	To be drafted to regulate UKE and NOVA relationship	UKE, NOVA	Q2/Q3 2026
Study A – Phase 4	N.6 - Privacy Notice	To be drafted	UKE, NOVA	Q2/Q3 2026
Study A – Phase 4	N.8 - DPIA	Planned	UKE, NOVA	Q2/Q3 2026
Study B	N.8 - DPIA	Planned	AUMC, RIGS, UKE	Q1 2026
Study B	N.1 - JCA	Review ongoing in UKE and RIGS	AUMC, UKE, RIGS	Q1 2026
Study B	N.6 - Privacy Notice	Draft ready, to be reviewed	AUMC, RIGS, UKE	Q1 2026
Study C	N.8 - DPIA	Planned (covered by Study B DPIA with specific section)	AUMC, RIGS, UKE	Q1 2026

Study C	N.1 - JCA	Review ongoing in UKE and RIGS	AUMC, UKE, RIGS	Q1 2026
Study C	N.6 - Privacy Notice	Draft ready, to be reviewed	AUMC, RIGS, UKE	Q1 2026
Study D	N.8 - DPIA	Planned	AUMC, RIGS, UKE	Q1 2026
Study D	N.1 - JCA	Review ongoing in UKE and RIGS	AUMC, UKE, RIGS	Q1 2026
Study D	N.6 - Privacy Notice	Draft ready, to be reviewed	AUMC, RIGS, UKE	Q1 2026
Study F	N.8 - DPIA	Planned (if needed)	UoC	Q4 2026
Study F	N.1 - JCA	Planned (specifically regarding DIGITALTWIN role)	UoC	Q4 2026

Study F	N.6 - Privacy Notice	Planned	UoC	Q4 2026
Website	N.1 - JCA / N.6 - PN	Update required due to switch from NURO to DIGITALTWIN	AUMC, DTT	Q1 2026
CMP	N.8 - DPIA / Risk Assessment	Planned (Milestone 7)	DTT	Month 24
CMP	N.6 - Privacy Notice / Cookie Policy	Planned	DTT	Before deployment

6. Annexed documentation

In this section we document the current versions of the GDPR documents that have been produced by CHINO in collaboration with all the involved responsible Partners.

Annex 1.1

RESEARCH PRIVACY NOTICE

Introduction

This Research Privacy Notice governs the use and storage of your personal data by the University of Limerick (the "University"). The processing of this data is carried out in accordance with the General Data Protection Regulation (GDPR) / Data Protection Acts 1988-2018 ("Data Protection Law") and in accordance with this Research Privacy Notice.

Any personal data which you provide to the University as part of this research project will be treated with the highest standards of security and confidentiality, in accordance with Irish and European Data Protection Law. This Notice sets out details of the information that we collect, how we process it and who we share it with. It also explains your rights under data protection law in relation to our processing of your data.

1. Title and Purpose of the research project .

1. **Title** : Burnout in hospital-based healthcare nursing and medical personnel

This research project is part of a larger research project, KEEPCARING, funded by the EU (grant no. 101137244, "the Project"). The KEEPCARING project aims to address the stress and burnout among healthcare professionals in the European Union. You can find the project's partner here.

Over the last several years burnout, i.e., emotional, physical and mental exhaustion has increased in healthcare workers globally including Ireland. This was made worse by COVID-19 pandemic where healthcare workers faced the brunt of the fallout of this while working at the coalface. This increase in burnout has resulted in poor mental and physical health, higher levels of fatigue, lower job satisfaction, as well as having a negative impact job recruitment and retention making a chronic situation even worse. This study aims to examine, via a survey, levels of burnout among hospital-based nursing and medical personal in several EU countries (starting with Ireland, Denmark, Germany and Netherlands) and to explore the determinants of this from an individual, social, management and systems level.

A sub-aim will be to give an option (tick box yes or no answer) to healthcare workers if they wanted to take part in future studies on burnout (e.g. have a one-to-one interview with us to elaborate on these experiences or if they wanted to or to wear a vest that monitors heart rates similar to a fit bit, i.e. non-invasively and unobtrusively without impacting your day-to-day work lives.)

The aim of this project is to understand levels of burnout in healthcare workers in the EU, and the factors that may be important in increasing or mitigating its risk. At the end of the research process, recommendations for good practice will be developed to raise better awareness of burnout in nursing and medical personnel and shape better work practices to alleviate the negative effects of burnout.

2. Research Ethics Committee

2.1 Ethical approval was granted by EHS Research Committee on [date to be added]. The research ethics approval number is [to be added].

3. Identity of the Data Controller(s)

3.1 The Data Controller

- University of Limerick, Plassey, Limerick.

4. Identity and Contact Details of the Data Protection Officer of the Data Controller(s)/

4.1 You can contact the University of Limerick's Data Protection Officer at dataprotection@ul.ie or by writing to Data Protection Officer, Room A1-073, University of Limerick, Limerick.

5. The Identity of the Principal Investigator

5.1 The Principal Investigator for this Research Project is Stephen Gallagher, Associate Professor in Psychology at the University of Limerick.

6. How we will use your personal data

6.1 The University must process personal data in order to undertake research relating to this project.

For this study, we are running an online survey and an interview study about burnout in healthcare workers groups. The research is using personal data to understand what the determinants and experiences of burnout in hospital-based nursing and medical personnel are. The survey is the main part of the study and it is completed without collecting directly identifiable information. We just use your IP address while you are completing the survey but we will not save this IP address, therefore once you have completed the survey we cannot identify you anymore. If you provide an email address because you choose to be contacted for the interview, we will be able to link your survey with your email address.

In addition, if you wish, you can also participate in future studies using non-invasive biomarkers such as heart rate, heart rate variability and breathing rate. In this case you will receive further information before starting the investigation.

6.2 Personal data collected and used for this survey is, for example: gender, age, work role and speciality, and ethnicity (aggregated for statistical information); some health-related personal data such as level of stress in the workplace.

7. Lawful Basis for University Processing Personal Data

7.1 Data Protection Law requires that the University must have a valid legal reason to process and use your personal data. This is often called a 'lawful basis'. GDPR requires us to be explicit with you about the lawful basis upon which we rely in order to process information about you.

7.2 The University is carrying out this research in the public interest and for scientific, historical or statistical purposes. In doing so, we are relying on Article 6(1)(e) of the GDPR. Where we are processing special category or sensitive personal data, we are relying on Article 9(2)(j) of GDPR. As required under Data Protection Law, we have appropriate safeguards in place in order to protect your personal data; these are set out in the next section.

8. Protecting Your Personal Data

8.1 We have the following measures in place to help ensure we keep your personal data safe:

- *All researchers at the University must adhere to University policies and procedures that tell our staff and students how to collect and use your information safely;*
- *Training is made available to all researchers to ensure our staff and students understand the importance of data protection and how to protect your personal data;*
- *The University has security arrangements and technical measures in place that ensure your information is stored safely and securely;*
- *All research projects involving personal data are reviewed and approved by a research ethics committee in line with University policies and procedures;*
- *Where a research project may involve a high risk, we first carry out a data protection impact assessment to assess risks and ensure adequate safeguards are in place;*

Further, our research partners at the Universidade NOVA de Lisboa, Portugal, University of Coimbra, Portugal, Copenhagen University Hospital, Rigshospitalet, Denmark, and Universitätsklinikum Hamburg-Eppendorf, Germany are joint data controllers abiding by these same regulations.

9. Sharing Your Personal Data with Third Parties

9.1 The University and KeepCaring Partners will not disclose your personal identifying information to third parties. We will share anonymous data with the partners of the Project for achieving the purposes of this Project. We may share anonymous and aggregated data with third parties for scientific research purposes.

10. Transfer of personal data to Other Countries Outside the EEA

We store the data in the EU. However, we rely on our suppliers Microsoft and Qualtrics which can have access to the data form outside the EU for the provision of some services. In this case, the transfer occurs in accordance with the safeguards set out in Chapter V of the GDPR (adequacy decision or, in the absence, on the basis of the Standard Contractual Clauses adopted by the EU Commission). If you wish to know more about these transfers please contact our DPO at Personal Data collected, dataprotection@ul.ie

11. How Long Will We Keep Your Data

11.1 Email addresses are stored for 36 months starting from the end of the survey. All research data will be kept for 7 years from the end of the survey.

12. Your Rights

12.1 You have the right to request that we:

- provide you with information as to whether we process your data and details relating to our processing, and with a copy of your personal data;
- rectify any inaccurate data we might have about your without undue delay;
- complete any incomplete information about you;
- under certain circumstances, erase your Personal Data without undue delay;
- under certain circumstances, be restricted from processing your data;
- Furnish you with the Personal Data which you provided us within a structured, commonly used and machine-readable format when the processing is based on the consent or on the contract.

You also have the right to object to the processing of your personal data.

12.2 Requests for any of the above should be addressed by email to the Principal Investigator at Stephen.gallagher@ul.ie and the Data Protection Officer at dataprotection@ul.ie. Your request will be processed within 30 days of receipt. Please note, however, it may not be possible to facilitate all requests, for example, where the University is required by law to collect and process certain personal data including that personal information that is required of any research participant.

12.3 It is your responsibility to let the Principal Investigator know if your contact details change.

13. Queries, Contacts, Right of Complaint

13.1 Further information on Data Protection at the University of Limerick may be viewed at www.ul.ie/dataprotection. You can contact the Data Protection Officer at dataprotection@ul.ie or by writing to Data Protection Officer, Room A1-073, University of Limerick, Limerick.

13.2 You have a right to lodge a complaint with the Office of the Data Protection Commissioner (Supervisory Authority). While we recommend that you raise any concerns or queries with us first at the following email address stephen.gallagher@ul.ie, you may contact that Office at info@dataprotection.ie or by writing to the Data Protection Commission, 21 Fitzwilliam Square South, Dublin 2, D02 RD28.

Annex 1.1.2

KEEPCARING

Privacy Notice for Research Study

Study A - Burnout in hospital-based healthcare nursing and medical personnel

Introduction

This Research Privacy Notice governs the use and storage of your personal data by the University of Limerick (the "University"). The processing of this data is carried out in accordance with the General Data Protection Regulation (GDPR) / Data Protection Acts 1988-2018 ("Data Protection Law") and in accordance with this Research Privacy Notice.

Any personal data which you provide to the University as part of this research project will be treated with the highest standards of security and confidentiality, in accordance with Irish and European Data Protection Law. This Notice sets out details of the information that we collect, how we process it and who we share it with. It also explains your rights under data protection law in relation to our processing of your data.

This research project is part of a larger research project, KEEPCARING, funded by the EU (grant no. 101137244, "the Project"). The KEEPCARING project aims to address the stress and burnout among healthcare professionals in the European Union. You can find the project's partner here (link).

Over the last several years burnout, i.e., emotional, physical and mental exhaustion has increased in healthcare workers globally including Ireland. This was made worse by COVID-19 pandemic where healthcare workers faced the brunt of the fallout of this

while working at the coalface. This increase in burnout has resulted in poor mental and physical health, higher levels of fatigue, lower job satisfaction, as well as having a negative impact job recruitment and retention making a chronic situation even worse.

Following Phase 1 of Study A with the online survey in which you took part, this part of study A aims to gather, via an interview, and later examine, views and experiences with burnout in the workplace.

Who will be using your data

The Data Controller is University of Limerick, Plassey, Limerick.

Data protection officer

You can contact the University of Limerick's Data Protection Officer at dataprotection@ul.ie or by writing to the Data Protection Officer, Room A1-073, University of Limerick, Limerick.

What personal data will be collected during this study

If you take part in the Study as volunteering healthcare professional working, we will collect the following personal data about you:

- **Identifying data** (e.g. name, surname)
- **Contact data** (e.g. email that you provided at the end of the online survey)
- **Opinions** (i.e. answers to the research questions and recordings of the interview). This might include health related data in the form of your personal experiences with stress and burn out.

Personal identifying information (e.g., name, contact details) is stored separately from the other research data and is accessible only to authorized members of the hospital. The key linking the identity of the participants with the study ID is kept securely and stored separately.

The recording and your transcript will be kept completely confidential. Only the research team will have access to the recording and transcript, and it will be anonymised.

Your de-identified data under the participants' ID will be stored on secure cloud storage with EU localisation (CASTOR and Zenodo).

Why do we process your data

We use the data to achieve the study's objective, as explained in the Introduction to the present document and in the information sheet of the Study.

Legal basis for processing your data

Your participation in this study is voluntary, and the data collected during this study is therefore based on your explicit consent, as collected at the end of the online survey in Phase 1. You express your consent through the consent form provided to you, where you can choose which of the activities with your data during or based on this study you agree with. You can agree with all or only some of the processing activities presented.

As stated in the information sheet, you can withdraw your consent at any time, without giving a reason. You can withdraw any or all the consents that you have given to processing of your personal data for this study at any time, without giving a reason. If you withdraw consent, we will stop collecting new data. Data already

collected and pseudonymized up to that point may continue to be used in the study if deletion would render the research impossible or seriously impair it. In this case, the data will be anonymized so it can no longer be linked to you.

Data recipients

We provide access to the data to our service providers which carry out some services on our behalf (such as IT services providers) as data processors in accordance with a data processing agreement.

We can communicate the data to other public or private bodies whenever we are obliged to do so to comply with law or regulatory requirements.

We will not disclose your personal data to any third party.

We will share anonymized data with the other partners of the Project for achieving the purposes of this Project. We may share anonymous and aggregated data with third parties for scientific research purposes.

We store your personal data in the EU. However, we might rely on suppliers based outside the EU (e.g. Microsoft) which can have access to the data for the provision of some services. In this case, the transfer occurs in accordance with the safeguards set out in Chapter V of the GDPR (adequacy decision or, in the absence, on the basis of the Standard Contractual Clauses adopted by the EU Commission). If you wish to know more about these transfers, please contact us.

How long we will keep your data

Data will be stored for 7 years after project's completion.

Your rights

You have certain rights in connection with the data processing.

- You have the right to access your data and to modify or correct your data.
- You can obtain the erasure of personal data and the restriction of the processing when certain conditions are met.
- You have the right to receive a copy of your personal data in a structured, commonly used and machine-readable format or ask Us to transmit that data to another controller, where technically feasible, if the processing is based on consent or on a contract and is carried out by automated means.
- You have the right to withdraw the consent you have given at any time, without affecting the lawfulness of the processing carried out before the withdrawal.
- You have a right to lodge a complaint with the Data Protection Supervisory Authority of your country.
- If you believe we are not processing your personal data in accordance with the law, you can complain to the Data protection Authority. A list of supervisory authorities with addresses can be found at this link.

Annex 1.1.3

Privacy Notice for Research Study:

Biomarker measurement in physicians and nursing staff on the general surgical ward: A pilot study on feasibility and acceptance

Version 1.0 dated 20/11/2025

As part of the Horizon Europe-founded project KEEPCARING, the Study "Biomarker measurement in physicians and nursing staff on the general surgical ward: A pilot study on feasibility and acceptance" (the "Study") aims to test whether measuring biomarkers with the Hexoskin vest is practical and acceptable for physicians and nursing staff on the general surgical ward during everyday clinical life.
As explained in the Participant Information Sheet, in order to achieve the goals of this study, personal data about you and your use of the Hexoskin will be collected and processed. The purpose of this document is to describe what data will be processed, by whom, for what purpose and under what conditions.

Who will be processing your data

This study is the joint effort of research teams of University Medical Center Hamburg-Eppendorf (UKE), Universidade NOVA de Lisboa (Portugal), University of Limerick (Ireland), University of Coimbra (Portugal), The Capital Region of Denmark (Region Hovedstaden), that are part of the KEEPCARING project https://keepcaring.eu/(the "Project").
These institutions are joint controllers responsible for processing of your data under this study.

What data will be collected during this study and how

Only the researchers from UKE and NOVA will know your name and surname, as explained in the information sheet. Everybody else involved in the study will only know your participant ID.
The following data will be collected:

- Continuous Electrocardiogram: ECG & Heart rate (HR), Heart rate variability (HRV), QRS events, Heart rate zones, maximum heart rate, resting heart rate, and heart rate recovery;
- Continuous thoracic and abdominal respiratory inductance plethysmography (RIP) sensors: Respiratory rate (RPM), Minute ventilation (L/min), and VO_2max;
- 3-axis Accelerometer: Activity intensity, maximum acceleration, steps, cadence, body positions;
- Questionnaire on marked stress events;
- AIM-FIM Scale;
- Questionnaire on subjective participant experiences;
- Stress levels.

This information will be linked with your participant ID and will be available to the study research teams.

Why is the data collected and processed

We use the data to achieve the Study's objective to evaluate the feasibility of measuring stress and resilience in healthcare workers during daily clinical activity on the ward using Hexoskin.
As we described in the Participant information sheet, this includes filling out burnout and resilience questionnaires as well as a questionnaire regarding your physical activity level, rating your stress level on a Visual Analog Scale (VAS) and collecting physiological biomarkers from the Hexoskin.

Legal basis for processing your data

Your participation in this study is voluntary and the data collected during this Study is based on your explicit consent.

This data is processed solely for scientific feasibility purposes. Individual data regarding your activity levels, stress, or body position will never be shared with your line managers or HR department and will not affect your employment evaluation.

You can withdraw the consent at any time, without giving a reason.

Where is your data and who can access your data

Your data will be collected in UKE and through the Hexoskin.

Personal identifying information (e.g., name, contact details) are stored separately from the other research data and are accessible only to authorized members of the hospital. The key linking the identity of the participants with the study ID is kept securely and stored separately.

Your de-identified data under the participants' ID will be stored on secure cloud storage with EU localisation (CASTOR for the questionnaires' data and Zenodo for long term storage).

This data will be accessed by

- the IT providers (storage and maintenance of the IT system) which act as processors under data processing agreements,
- the study research teams of the Join controllers from EU States.

Data could be further accessed by regulators, whose job it is to check the work of researchers.

The results of the study will be published in an anonymous or aggregated manner.

We store your data in Europe. However, some of our suppliers, when providing their services, can access data from countries outside of the EU/EEA, such as Hexoskin (from the US). In these cases, data is transferred only in the presence of the

safeguards indicated in the applicable data protection legislation. In particular, the transfer will take place: – to destination countries for which the European Commission has issued an adequacy decision (art. 45 GDPR) or – on the basis of the Standard contractual clauses ("SCCs") adopted by the EU Commission (art. 46 GDPR) provided that supplementary security measures are also in place.

How long will your data be kept

Your de-identified data from the Hexoskin usage and questionnaires will be retained by the joint controllers for five years after the end of the Study.

What are your rights?

- You can request access to the data we process about you.
- If at any point you believe that the data we process relating to you is incorrect, you can contact us, and we will verify and correct the data.
- If certain conditions are met you can obtain the restriction of the processing of your data or the erasure.
- If technically feasible, you can also exercise your right to data portability regarding the data that is processed automatically.
- You can withdraw the consent that you have given to the processing of your personal data for this Study at any time, without giving a reason. If you withdraw from the study or withdraw your consent, your data will be anonymised or erased, unless agreed otherwise.

If you wish to exercise any of these rights, please contact the the hospital Data Protection Officer at UKE:

Matthias Jaster Martinistraße 52 20246 Hamburg Tel. 040/7410 56890 E-Mail: dsb@uke.de

If you believe we are not processing your personal data in accordance with the law, you can complain to the Data protection Authority.

A list of supervisory authorities with addresses can be found at: https://www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html.

Responsible for the UKE is: The Hamburg Commissioner for Data Protection and Freedom of Information Ludwig-Erhard-Straße 22 20459 Hamburg Tel.: 040/42854-4040 Fax.: 040/42854-4000 mailbox@datenschutz.hamburg.de https://www.datenschutz-hamburg.de/

Annex 1.2

KEEPCARING

Privacy Notice for Research Study

Study B - Deep relaxation using Virtual Reality intervention before surgery for healthcare professionals working in the operating room

Version: 1.0 - 24/11/2025

Introduction

As part of the Horizon Europe-founded project KEEPCARING (the "Project"), this study aims to better understand if, and to what extent, a Virtual Reality (VR) intervention can help to reduce stress in the workplace. We will look at how people experience their stress (via questionnaires) before and after the intervention, but also at physical signals of stress, such as heart rate and heart rate variability. We are comparing the effects of the VR headset with those of a quiet (low-stimulus) environment. Additionally, we are investigating how satisfied participants are with both interventions.

As explained in the Participant Information Sheet, in order to achieve the goals of this study, personal data about you will be collected and processed. The purpose of this document is to describe what data will be processed, by whom, for what purpose and under what conditions.

Who will be using your data

As partners in the Project and as part of the tasks of Work Package 3,

- Amsterdam University Medical Centers at the University of Amsterdam (AUMC)
- University Medical Center Hamburg-Eppendorf (UKE)
- Rigshospitalet (RIGS)

are joint controllers and they are jointly responsible for the processing of your personal data. They all have appointed a DPO (see Contact addresses at the end of this document).

What personal data will be collected during this study

If you take part in the Study as healthcare professional working in one of the three Hospitals listed above, we will collect the following personal data about you:

Data categories	Examples of Data items	Data subjects
Identification data	Name, Surname	Health care professionals employed in the operating rooms of the three Parties' University Hospitals or other participating hospitals
Contact data	Email	
Demographic data	Sex, Age	
Professional data	Profession, Hospital, Specialty, Country, Work experience, Workhours per workweek	
Usage data	Type of VR environment chosen and VR environment changes in correlation with measured heart rate	

Non-invasive biomarkers *Health data under Art. 9 GDPR. Measured and calculated by POLAR H1*	Heart rate, Heart rate variability	
Prescription of medications *Health data under Art. 9 GDPR*	Medication use for symptoms of anxiety, stress and-or depression	
Opinions *May constitute Health data under Art. 9 GDPR*	Questionnaire answers related to several relevant topics, among which: Perceived stress level, Satisfaction with the intervention	
Habits	Smoking habits, sleep patterns	
Analysed data *Health data under Art. 9 GDPR*	Correlation between perceived stress and non-invasive biomarkers, Association between baseline characteristics (e.g. demographic data) and stress	

All data will be pseudonymized (coded). We assign a code to your data. The key to the code is stored securely in the hospital, which collects the data. Only the researcher and authorized team members know the codes. Participants can be identified in the database by their ID number. The participants identification log will be kept separate from the participant data and will be safeguarded by the local principal investigator. For the participating centers, a separate site-specific subject identification log will be kept at each study site. In other words, personal identifying information (e.g., name, contact details) are stored separately from the other research data and are accessible only to authorized members of the hospital. The key linking the identity of the participants with the study ID is kept securely and stored separately.

Your de-identified data under the participants' ID will be stored on secure cloud storage with EU localisation (CASTOR and Zenodo).

Why do we process your data

We use the data to achieve the study's objective, as explained in the Introduction to the present document and in the information sheet of the Study.

Legal basis for processing your data

Your participation in this study is voluntary, and the data collected during this study is therefore based on your explicit consent. As this research involves employees, please be assured that your decision to participate - or not to participate - will have no impact on your employment, performance evaluations, or professional standing.

You express the extent of your consent through the consent form provided to you, where you can choose which of the activities with your data during or based on this

study you agree with. You can agree with all or only some of the processing activities presented.

As stated in the information sheet, withdrawal from the Study will have absolutely no impact on your employment status or professional relationship.

You can withdraw any or all the consents that you have given to processing of your personal data for this study at any time, without giving a reason. If you withdraw consent, we will stop collecting new data. Data already collected and pseudonymized up to that point may continue to be used in the study if deletion would render the research impossible or seriously impair it. In this case, we will make sure the data can no longer be linked to you.

Data recipients

We provide access to the data to our service providers which carry out some services on our behalf (such as IT services providers) as data processors in accordance with a data processing agreement.

We can communicate the data to other public or private bodies whenever we are obliged to do so to comply with law or regulatory requirements.

We will not disclose your personal identifying information to other third parties. The Joint Controllers will have access to the pseudonymized data (coded data) of all the sites involved in the Study.

We will share anonymized data with the other partners of the Project for achieving the purposes of this Project. We may share anonymous and aggregated data with third parties for scientific research purposes.

Please also note that the provider of the VR system won't have any access to the data, which will only be accessible by the researchers.

How long we will keep your data

Data will be stored for 5 years after project's completion.

Your rights

- You have certain rights in connection with the data processing.
- You have the right to access your data and to modify or correct your data.
- You can obtain the erasure of personal data and the restriction of the processing when certain conditions are met.
- You have the right to receive a copy of your personal data in a structured, commonly used and machine-readable format or ask Us to transmit that data to another controller, where technically feasible, if the processing is based on consent or on a contract and is carried out by automated means.
- You have the right to withdraw the consent you have given at any time, without affecting the lawfulness of the processing carried out before the withdrawal.
- You have a right to lodge a complaint with the Data Protection Supervisory Authority of your country.
- The Joint controllers have signed a joint controllership agreement and you can receive an abstract of this agreement by contacting them at the email addresses indicated below.

Contacts address

If you wish to exercise one of these rights or contact the joint controllers, you can write at

AUMC: privacy@amsterdamumc.nl;

UKE: dsb@uke.de;

RIGS: forskningsjura.rigshospitalet@regionh.dk.

If you believe we are not processing your personal data in accordance with the law, you can complain to the Data protection Authority.

A list of supervisory authorities with addresses can be found at this link.

Annex 1.3

KEEPCARING

Privacy Notice for Research Study

Study C - Evaluating Healthcare Professionals' Satisfaction and Stress Mitigation Using Virtual Reality Intervention in Surgical Ward: a multination feasibility study

Version: 1.0 - 24/11/2025

Introduction

As part of the Horizon Europe-founded project KEEPCARING (the "Project"), this study aims to gain insight into the feasibility, acceptance, and satisfaction of healthcare professionals on surgical wards regarding a Virtual Reality (VR) intervention.

We are looking at user comfort and studying how VR can best be integrated into daily practice. Additionally, we are investigating the effect of the intervention on the perceived stress level before and after using VR.

As explained in the Participant Information Sheet, in order to achieve the goals of this study, personal data about you will be collected and processed. The purpose of this document is to describe what data will be processed, by whom, for what purpose and under what conditions.

Who will be using your data

As partners in the Project and as part of the tasks of Work Package 3,

- Amsterdam University Medical Centers at the University of Amsterdam (AUMC)

- University Medical Center Hamburg-Eppendorf (UKE)
- Rigshospitalet (RIGS)

are joint controllers and they are jointly responsible for the processing of your personal data. They all have appointed a DPO (see Contact addresses at the end of this document).

What personal data will be collected during this study

If you take part in the Study as healthcare professional working in one of the three Hospitals listed above, we will collect the following personal data about you:

Data categories	Data items	Data subjects
Identification data	Name, Surname	Health care professionals employed in the surgical wards of the three Parties' University Hospitals or other participating hospitals
Contact data	Email	
Demographic data	Sex, Age	
Professional data	Profession, Hospital, Specialty, Country, Work experience, Workhours per workweek	
Usage data	Type of VR environment chosen and VR environment changes	

Opinions	Questionnaire answers related to a number of relevant topics, among which: Perceived stress before and after the VR intervention, Satisfaction with the intervention, User comfort (CyberSickness in Virtual Reality Questionnaire (CSQ-VR)), comfort with perceived complexity, Perceived disadvantages, Personal emotion, Social influence, Perceived advantages	
Analysed data	Statistical analysis of the collected data points, Association between baseline characteristics (e.g. demographic data) and user satisfaction	
Interview Data	Audio recordings of the interview; Transcripts of the conversation.	Applies only to the 5 participants selected for optional follow-up.

All data will be pseudonymized (coded). We assign a code to your data. The key to the code is stored securely in the hospital, which collects the data. Only the researcher

and authorized team members know the codes. Participants can be identified in the database by their ID number. The participants identification log will be kept separate from the participant data and will be safeguarded by the local principal investigator. For the participating centers, a separate site-specific subject identification log will be kept at each study site. In other words, personal identifying information (e.g., name, contact details) are stored separately from the other research data and are accessible only to authorized members of the hospital. The key linking the identity of the participants with the study ID is kept securely and stored separately.

Your de-identified data under the participants' ID will be stored on secure cloud storage with EU localisation (CASTOR and Zenodo).

We will transcribe the audio recordings. After this, the recording itself will be destroyed immediately upon verification of the transcript. The transcript itself will be pseudonymized (names removed, if any) so the text data can be kept safely.

Why do we process your data

We use the data to achieve the study's objective, as explained in the Introduction to the present document and in the information sheet of the Study.

Legal basis for processing your data

Your participation in this study is voluntary, and the data collected during this study is therefore based on your explicit consent. As this research involves employees, please be assured that your decision to participate - or not to participate - will have no impact on your employment, performance evaluations, or professional standing.

You express the extent of your consent through the consent form provided to you, where you can choose which of the activities with your data during or based on this study you agree with. You can agree with all or only some of the processing activities presented.

As stated in the information sheet, withdrawal from the Study will have absolutely no impact on your employment status or professional relationship.

You can withdraw any or all the consents that you have given to processing of your personal data for this study at any time, without giving a reason. If you withdraw consent, we will stop collecting new data. Data already collected and pseudonymized up to that point may continue to be used in the study if deletion would render the research impossible or seriously impair it. In this case, we will make sure the data can no longer be linked to you.

Data recipients

We provide access to the data to our service providers which carry out some services on our behalf (such as IT services providers) as data processors in accordance with a data processing agreement.

We can communicate the data to other public or private bodies whenever we are obliged to do so to comply with law or regulatory requirements.

We will not disclose your personal identifying information to other third parties. The Joint Controllers will have access to the pseudonymized data (coded data) of all the sites involved in the Study.

We will share anonymized data with the other partners of the Project for achieving the purposes of this Project. We may share anonymous and aggregated data with third parties for scientific research purposes.

Please also note that the provider of the VR system won't have any access to the data, which will only be accessible by the researchers.

How long we will keep your data

Data will be stored for 5 years after project's completion.

Your rights

- You have certain rights in connection with the data processing.
- You have the right to access your data and to modify or correct your data.
- You can obtain the erasure of personal data and the restriction of the processing when certain conditions are met.
- You have the right to receive a copy of your personal data in a structured, commonly used and machine-readable format or ask Us to transmit that data to another controller, where technically feasible, if the processing is based on consent or on a contract and is carried out by automated means.
- You have the right to withdraw the consent you have given at any time, without affecting the lawfulness of the processing carried out before the withdrawal.
- You have a right to lodge a complaint with the Data Protection Supervisory Authority of your country.
- The Joint controllers have signed a joint controllership agreement and you can receive an abstract of this agreement by contacting them at the email addresses indicated below.

Contacts address

If you wish to exercise one of these rights or contact the joint controllers, you can write at

AUMC: privacy@amsterdamumc.nl;

UKE: dsb@uke.de;

RIGS: forskningsjura.rigshospitalet@regionh.dk.

If you believe we are not processing your personal data in accordance with the law, you can complain to the Data protection Authority.

A list of supervisory authorities with addresses can be found at this link.

Annex 1.4

KEEPCARING

Privacy Notice for Research Study

Longer term resilience Team debriefing after surgery

As part of the Horizon Europe-founded project KEEPCARING (the "Project"), this Study aims to evaluate the impact of structured postoperative debriefings with and without procedural, structured audio- and video recordings, on team performance, psychological safety, and non-technical skills in the operating room.

As explained in the Participant Information Sheet, in order to achieve the goals of this study, personal data about you will be collected and processed. The purpose of this document is to describe what personal data will be processed, by whom, for what purpose and under what conditions.

Who will be using your data

As partners in the Project and as part of the tasks of Work Package 3,

- Amsterdam University Medical Centers at the University of Amsterdam (AUMC)
- University Medical Center Hamburg-Eppendorf (UKE)
- Rigshospitalet (RIGS)

are joint controllers and they are jointly responsible for the processing of your personal data.

You can contact us at any time using the following contact details:

AUMC: privacy@amsterdamumc.nl

UKE: dsb@uke.de

RIGS: forskningsjura.rigshospitalet@regionh.dk.

What personal data will be collected during this study

If you take part in the Study as healthcare professional working in one of the three Hospitals listed above, we will collect the following personal data about you:

- **Identification data** (Name, Surname);
- **Contact data** (Email);
- **Observational data of the team debriefing**, including detailed field notes documenting, among others, team members' engagement levels, communication styles, decision-making processes, conflict resolution approaches, and the interpersonal nuances that emerge during collaborative discussions;
- **Observational data through the ORBB** (**AUMC and RIGS**), e.g. real-time video and audio recordings of surgical procedures performed by the OR team;
- **Opinions**, such as data collected via self-reported measurements through questionnaires and qualitative interviews and audio recordings of the interviews.

All data will be pseudonymized (coded). We assign a code to your data. The key to the code is stored securely in the hospital, which collects the data. Only the researcher and authorized team members know the codes. Participants can be identified in the database by their ID number. The participation identification log will be kept separate

from the participant data and will be safeguarded by the local principal investigator. For the participating centers, a separate site-specific subject identification log will be kept at each study site. In other words, personal identifying information (e.g., name, contact details) are stored separately from the other research data and are accessible only to authorized members of the hospital. The key linking the identity of the participants with the study ID is kept securely and stored separately.

Why do we process your data

We use the data to achieve the study's objective, as explained in the Introduction to the present document and in the information sheet of the Study.

Legal basis for processing your data

Your participation in this study is voluntary, and the data collected during this study is therefore based on your explicit consent. As this research involves employees, please be assured that your decision to participate - or not to participate - will have no impact on your employment, performance evaluations, or professional standing.

You express the extent of your consent through the consent form provided to you, where you can choose which of the activities with your data during or based on this study you agree with. You can agree with all or only some of the processing activities presented.

As stated in the information sheet, withdrawal from the Study will have absolutely no impact on your employment status or professional relationship.

You can withdraw any or all the consents that you have given to processing of your personal data for this study at any time, without giving a reason. If you withdraw consent, we will stop collecting new data. Data already collected and pseudonymized up to that point may continue to be used in the study if deletion would render the research impossible or seriously impair it. In this case, we will make sure the data can no longer be linked to you.

Data recipients

We provide access to the data to our service providers which carry out some services on our behalf (such as IT services providers) as data processors in accordance with a data processing agreement.

We can communicate the data to other public or private bodies whenever we are obliged to do so to comply with law or regulatory requirements.

We will not disclose your personal identifying information to other third parties. We will share anonymized data with the other partners of the Project for achieving the purposes of this Project. We may share anonymous and aggregated data with third parties for scientific research purposes.

We store your personal data in the EU. However, we might rely on suppliers based outside the EU (for IT services and secure storage) which can have access to the data for the provision of some services. Moreover, we rely on Surgical Safety Technologies Inc as provider of the ORBB system, which is based in Canada and can access the data through the cloud system in use. In these cases, the transfer occurs in accordance with the safeguards set out in Chapter V of the GDPR (adequacy

decision or, in the absence, on the basis of the Standard Contractual Clauses adopted by the EU Commission). If you wish to know more about these transfers, please contact us.

How long we will keep your data

Data will be held for 10 years.

Your rights

- You have certain rights in connection with the data processing.
- You have the right to access your data and to modify or correct your data.
- You can obtain the erasure of personal data and the restriction of the processing when certain conditions are met.
- You have the right to receive a copy of your personal data in a structured, commonly used and machine-readable format or ask Us to transmit that data to another controller, where technically feasible, if the processing is based on consent or on a contract and is carried out by automated means.
- You have the right to withdraw the consent you have given at any time, without affecting the lawfulness of the processing carried out before the withdrawal.
- You have a right to lodge a complaint with the Data Protection Supervisory Authority of your country.
- The Joint controllers have signed a joint controllership agreement and you can receive an abstract of this agreement by contacting them at the email addresses indicated below.

Contacts address

If you wish to exercise one of these rights or contact the joint controllers, you can write at

AUMC: privacy@amsterdamumc.nl;

UKE: dsb@uke.de;

RIGS: forskningsjura.rigshospitalet@regionh.dk.

If you believe we are not processing your personal data in accordance with the law, you can complain to the Data protection Authority.

A list of supervisory authorities with addresses can be found at this link.

Annex 1.5.1

KEEPCARING

STUDY E - "Co-work design: A structural approach to reduce individual work stress in healthcare professionals in hospital settings"

PRIVACY NOTICE

1. **Introduction**

This Privacy Notice governs the processing and storage of your personal data in the Study, "*Co-work design: A structural approach to reduce individual work stress in healthcare professionals in hospital settings" (*hereinafter, "the Study", "Study"*).*

This Study is part of a larger project, KEEPCARING, funded by the EU (hereinafter the "KEEPCARING project"; "the project"). The project (project no. 101137244) aims to address stress and burnout among healthcare professionals in the European Union. You can find out more about the project here.

You are reading this document because you have expressed to your Hospital the interest in taking part in the Study. Any personal data which you provide to us as part of this Study will be treated with the highest standards of security and confidentiality, in accordance with the European Data Protection Law and the applicable local laws. This Notice sets out details of the information that we collect, how we process it and who we share it with. It also explains your rights under data protection law in relation to our processing of your data.

2. **What is the Study about?**

As partner in the KEEPCARING project,

- ERASMUS UNIVERSITEIT ROTTERDAM, established in BURGEMEESTER OUDLAAN 50, ROTTERDAM 3062 PA, Netherlands [EUR]

we are organizing a Study, in the context of Work Package 4, to gain insight into your experiences in the workplace and the extent to which you and your colleagues are able to shape your work together. This is known as co-work design. The insights from this Study will help us develop and evaluate an intervention to reduce work-related stress among hospital nurses.

The Study received the approval of EUR's Ethics Committee as Ethics Application ETH2425-0324.

3. **Identity of the Data Controller**

EUR is the data controller of your personal data. This means that EUR is responsible for the collection and processing of your personal data in the context of the Study. You can contact us at any time using the following contact details: solms@essb.eur.nl.

4. **Identity and Contact Details of the Data Protection Officer**

We have appointed a Data Protection Officer ("**DPO**") who is responsible for overseeing our privacy practices and our compliance with applicable data protection laws. You can contact our DPO via email, by writing to fg@eur.nl.

5. **How we will collect and use your personal data**

The Study consists of two phases. In the first phase, we ask you to complete a questionnaire with general questions about yourself and your work. This questionnaire will take approximately 10–15 minutes to complete. The second phase is a diary study, in which you will complete a short daily questionnaire over 2 weeks. These questionnaires focus on your daily experiences at work. Completing this daily questionnaire will take about 5 minutes. You will be asked to complete the questionnaires using a dedicated online platform (QUALTRICS).

In the following table you can find the list of personal data that we will collect and analyze through the questionnaires.

Data categories	Examples of Data items	Data subjects
Identification data	Name	Nurses
Contact data	Email address (provided by your Hospital)	
Demographic data	Age, Gender	
Navigation data	IP address, other digital identifiers used by QUALTRICS to administer the questionnaires	
Information about your personal work situation and your experiences at work	Job tenure, Role tenure, Job title, Specialty, Ward, Employment status, Overtime, Team size	
Measured variables in daily surveys (Responses to the questionnaires) *These responses may qualify as special categories of personal data (art. 9 GDPR).*	Prosocial job crafting, Exchange of resources, Burnout, Work engagement, and flourishing, Psychological capital, Workload	

We do not process Personal Data for automated decision-making activities or profiling.

6. **Purpose of the processing and legal basis**

As stated, the purpose of this Study is to gain insight into your experiences in the workplace and the extent to which you and your colleagues are able to shape your work together. To pursue this purpose, we need to process your personal data.

Participation in the study is completely voluntary. This means that you decide if you want to participate and provide us with your personal data for the purpose of conducting the Study. Consequently, we are relying on Article 6(1)(a) GDPR, i.e. your consent as a legal basis for the processing of your personal data. Where we are processing special categories of personal data (e.g. health related data, etc.), we are relying on Article 9(2)(a) GDPR, i.e. your explicit consent. You can withdraw your consent at any time by contacting us at solms@essb.eur.nl.

7. Protecting your personal data

Data collection and processing in the Study will follow a structured approach to ensure security, confidentiality, and compliance with data protection regulations.

Data security, storage and access

All data collected during the Study will be handled with the highest regard for participant privacy.

Data will be securely stored in a restricted-access account on QUALTRICS, accessible only to the Data Controller.

Each participant will be assigned a unique alphanumeric code to facilitate the analysis while maintaining anonymity. This unique code will not contain any personally identifiable information, and it will be used to link responses to data within the Study activities. This unique code will be accessible only to EUR's team.

8. Data sharing

Your responses will be treated confidentially and will never be shared with your colleagues, supervisor, or others. In scientific articles, we will only use anonymized results.

We will not disclose your personal identifying information to third parties. We will share anonymized data with the other partners of the KEEPCARING Project for achieving the purposes of the project. We may share anonymous and aggregated data with third parties for scientific research purposes.

However, if, and only if, you have consented to your employer receiving pseudonymized data from your questionnaire responses, we will share your responses with them. In this case, we will not associate your email address, name, or other directly identifiable data with your responses. Your responses will be analyzed by a dedicated research team. The responses will only be linked to your unique ID. However, given the type of topics addressed in your questionnaire, your employer may still be able to indirectly identify you. Please be aware that even if this occurs, there will be no negative consequences for you.

Moreover, we ensure that our suppliers, acting as Data Processors (such as IT services' providers), will only process your personal data to provide their services under appropriate confidentiality and security obligations and in accordance with our instructions and with this Policy.

9. Transfer of personal data to Other Countries Outside the EEA

We store your personal data in the EU. However, we might rely on suppliers based outside the EU (e.g. Qualtrics) which can have access to the data for the provision of some services. In this case, the transfer occurs in accordance with the safeguards set out in Chapter V of the GDPR (adequacy decision or, in the absence, on the basis of the Standard Contractual Clauses adopted by the EU Commission). If you wish to know more about these transfers, please contact us.

10. How long we will keep your data

Data will be collected, analyzed, and stored by the Data Controller for the duration of the KEEPCARING project plus 10 years.

11. **Your rights**

You have the right to request that we:

- provide you with information as to whether we process your data and details relating to our processing, and with a copy of your personal data;
- rectify any inaccurate data we might have about you without undue delay;
- complete any incomplete information about you;
- under certain circumstances, erase your Personal Data without undue delay;
- under certain circumstances, be restricted from processing your data;
- furnish you with the Personal Data which you provided us within a structured, commonly used and machine-readable format when the processing is based on the consent or on the contract.

You can withdraw your consent at any time. Please, keep in mind that the withdrawal will not affect the lawfulness of processing based on consent before its withdrawal.

Requests for any of the above should be addressed by email to solms@essb.eur.nl and fg@eur.nl. Your request will be processed within 30 days of receipt. Please note, however, it may not be possible to facilitate all requests, for example, where EUR is required by law to collect and process certain personal data including that personal information that is required of any research participant.

It is your responsibility to let the Principal Investigator know if your contact details change.

You have a right to lodge a complaint with the Office of the Data Protection Supervisory Authority of your country.

Last updated

05/09/2025

Annex 1.5.2

KEEPCARING

STUDY E - "Co-work design: A structural approach to reduce individual work stress in healthcare professionals in hospital settings"

PRIVACY NOTICE

1. **Introduction**

This Privacy Notice governs the processing and storage of your personal data in the Study, "*Co-work design: A structural approach to reduce individual work stress in healthcare professionals in hospital settings" (*hereinafter, "the Study", "Study"*).*

This Study is part of a larger project, KEEPCARING, funded by the EU (hereinafter the "KEEPCARING project"; "the project"). The project (project no. 101137244) aims to address stress and burnout among healthcare professionals in the European Union. You can find out more about the project here.

You are reading this because you have been invited to share your email address to take part in the Study. This Notice sets out details of the information that we collect, how we process it and who we share it with. It also explains your rights under data protection law in relation to our processing of your data.

2. **What is the Study about?**

As partner in the KEEPCARING project,

- ERASMUS UNIVERSITEIT ROTTERDAM, established in BURGEMEESTER OUDLAAN 50, ROTTERDAM 3062 PA, Netherlands [EUR]

is organizing a Study to gain insight into your experiences in the workplace and the extent to which you and your colleagues are able to shape your work together. This is known as

co-work design. The insights from this Study will help EUR develop and evaluate an intervention to reduce work-related stress among hospital nurses.

The Study received the approval of EUR's Ethics Committee as Ethics Application ETH2425-0324.

3. **Identity of the Data Controller**

[Insert identity of the data controller – i.e. the participating hospital] is the data controller of your personal data for the processing activity indicate below and is thus responsible for the collection and processing of your personal data. You can contact us at any time using the following contact details: [Insert contact details].

4. **Identity and Contact Details of the Data Protection Officer**

We have appointed a Data Protection Officer ("**DPO**") who is responsible for overseeing our privacy practices and our compliance with applicable data protection laws. You can contact our DPO via email, by writing to [Insert DPO's contact details].

5. **How we will collect and use your personal data**

The Study consists of two phases. In the first phase, you will be asked to complete a questionnaire with general questions about yourself and your work. This questionnaire will take approximately 10–15 minutes to complete. The second phase is a diary study, in which you will complete a short daily questionnaire over 2 weeks. These questionnaires focus on your daily experiences at work. Completing this daily questionnaire will take about 5 minutes. You will be contacted by EUR and you will be asked to complete the questionnaires using a dedicated online platform (QUALTRICS).

In the following table you can find the list of personal data that we will collect and that we will share with EUR to allow you to sign up for the Study.

Data categories	Examples of Data items	Data subjects
Identification data	Name	Nurses
Contact data	Email address	

We do not process special categories of personal data (aka "sensitive data", such as health data, political opinions, etc.) or any other personal data different form what we have identified above.

We do not process Personal Data for automated decision-making activities or profiling.

6. **Purpose of the processing, data sharing and legal basis**

As previously mentioned, we are collecting your personal data to share it with EUR, enabling your participation in the Study. This purpose requires us to process your personal data.

Participation in the study is completely voluntary. This means that you decide if you want to participate and provide us with your personal data for the purpose of sharing it with EUR. Consequently, we are relying on Article 6(1)(a) GDPR, i.e. your consent as a legal basis for the processing of your personal data. You can withdraw your consent at any time by contacting us at [Insert contact details].

7. **Data sharing**

Your personal data will be shared with EUR, to enable you to sign up to participate in the Study.

Moreover, we ensure that our suppliers, acting as Data Processors (such as IT services' providers), will only process your personal data to provide their services under appropriate confidentiality and security obligations and in accordance with our instructions and with this Policy.

8. **Transfer of personal data to Other Countries Outside the EEA**

We store your personal data in the EU. However, we might rely on suppliers based outside the EU which can have access to the data for the provision of some services. In this case, the transfer occurs in accordance with the safeguards set out in Chapter V of the GDPR (adequacy decision or, in the absence, on the basis of the Standard Contractual Clauses adopted by the EU Commission). If you wish to know more about these transfers, please contact us.

9. **How long we will keep your data**

Once EUR confirms that your data has been correctly received, we will delete it from our systems and stop processing it for the aforementioned purpose.

10. **Your rights**

You have the right to request that we:

- provide you with information as to whether we process your data and details relating to our processing, and with a copy of your personal data;
- rectify any inaccurate data we might have about you without undue delay;
- complete any incomplete information about you;
- under certain circumstances, erase your Personal Data without undue delay;
- under certain circumstances, be restricted from processing your data;
- furnish you with the Personal Data which you provided us within a structured, commonly used and machine-readable format when the processing is based on the consent or on the contract.

You can withdraw your consent at any time. Please, keep in mind that the withdrawal will not affect the lawfulness of processing based on consent before its withdrawal.

Requests for any of the above should be addressed by email to [Insert contact details]. Your request will be processed within 30 days of receipt. Please note, however, it may not be possible to facilitate all requests, for example, where EUR is required by law to collect and process certain personal data including that personal information that is required of any research participant.

It is your responsibility to let the Principal Investigator know if your contact details change.

You have a right to lodge a complaint with the Office of the Data Protection Supervisory Authority of your country.

Last updated

05/09/2025

Annex 1.5.3

KEEPCARING

STUDY E - "Co-work design: A structural approach to reduce individual work stress in healthcare professionals in hospital settings"

PRIVACY NOTICE

1. Introduction

This Research Privacy Notice governs the processing and storage of your personal data in the Study, "*Co-work design: A structural approach to reduce individual work stress in healthcare professionals in hospital settings" (*hereinafter, "the Study", "Study"*).*

This Study is part of a larger project, KEEPCARING, funded by the EU (hereinafter the "KEEPCARING project"; "the project"). The project (project no. 101137244) aims to address stress and burnout among healthcare professionals in the European Union. You can find out more about the project here.

You are reading this because you have been invited to share your email address to take part in the Study. Any personal data which you provide to us will be treated with the highest standards of security and confidentiality, in accordance with the European Data Protection Law and the applicable local laws. This Notice sets out details of the information that we collect, how we process it and who we share it with. It also explains your rights under data protection law in relation to our processing of your data.

2. What is the Study about?

As partner in the KEEPCARING project,

- ERASMUS UNIVERSITEIT ROTTERDAM, established in BURGEMEESTER OUDLAAN 50, ROTTERDAM 3062 PA, Netherlands [EUR]

is organizing a Study to gain insight into your experiences in the workplace and the extent to which you and your colleagues are able to shape your work together. This is known as co-work design. The insights from this Study will help EUR develop and evaluate an intervention to reduce work-related stress among hospital nurses.

The Study received the approval of EUR's Ethics Committee as Ethics Application ETH2425-0324.

3. **Identity of the Data Controller**

[Insert identity of the data controller – i.e. the participating hospital] is the data controller of your personal data and is thus responsible for the collection and processing of your personal data. You can contact us at any time using the following contact details: [Insert contact details].

4. **Identity and Contact Details of the Data Protection Officer**

We have appointed a Data Protection Officer ("**DPO**") who is responsible for overseeing our privacy practices and our compliance with applicable data protection laws. You can contact our DPO via email, by writing to [Insert DPO's contact details].

5. **How we will collect and use your personal data**

The Study consists of two phases. In the first phase, you will be asked to complete a questionnaire with general questions about yourself and your work. This questionnaire will take approximately 10–15 minutes to complete. The second phase is a diary study, in which you will complete a short daily questionnaire over 2 weeks. These questionnaires focus on your daily experiences at work. Completing this daily questionnaire will take about 5 minutes. You will be contacted by EUR and you will be asked to complete the questionnaires using a dedicated online platform (QUALTRICS).

In the following table you can find the list of personal data that we will collect and that we will share with EUR to allow you to sign up for the Study.

Data categories	Examples of Data items	Data subjects
Identification data	Name	Nurses
Contact data	Email address	
Responses data **(pseudonymized)** *These responses may qualify as special categories of personal data (art. 9 GDPR).*	Questionnaires responses	

We do not process Personal Data for automated decision-making activities or profiling.

6. **Purpose of the processing, data sharing and legal basis**

i. **Enabling your participation in the Study**

As previously mentioned, we are collecting and processing your personal data to share it with EUR, enabling your participation in the Study. This purpose requires us to process your personal data.

Participation in the study is completely voluntary. This means that you decide if you want to participate and provide us with your personal data for the purpose of sharing your data with EUR. Consequently, we are relying on Article 6(1)(a) GDPR, i.e. your consent as a legal basis for the processing of your personal data.

ii. **Questionnaires' responses analysis**

We would like to get the responses you give to the EUR questionnaires. This will help us analyze the data for our hospital, so we can improve the well-being of our staff. The responses won't include any direct identifying information, like your name or email. They will only be linked to the anonymous ID that EUR gives you when you sign up. We can't connect this ID to your identity. However, because of the type of information in the responses, it might be possible to indirectly identify you. We will not use this data to penalize you in any way.

It is your choice whether or not to let us have your responses. Because of this, we are using your consent as the legal basis for processing your data under the GDPR:

- For personal data, we are relying on Article 6(1)(a) GDPR, which is your specific consent.
- For special categories of personal data, such as health information, we are relying on Article 9(2)(a) GDPR, which is your explicit consent.

6.i and 6.ii are two separate consents. You can still participate in the study even if you decide not to consent to 6.ii.

You can withdraw your consent at any time by contacting us at [Insert contact details].

9. **Data sharing**

Your personal data will be shared with EUR, to enable you to sign up to participate in the Study.

Moreover, we ensure that our suppliers, acting as Data Processors (such as IT services' providers), will only process your personal data to provide their services under appropriate confidentiality and security obligations and in accordance with our instructions and with this Policy.

10. **Transfer of personal data to Other Countries Outside the EEA**

We store your personal data in the EU. However, we might rely on suppliers based outside the EU which can have access to the data for the provision of some services. In this case, the transfer occurs in accordance with the safeguards set out in Chapter V of the GDPR (adequacy decision or, in the absence, on the basis of the Standard Contractual Clauses adopted by the EU Commission). If you wish to know more about these transfers, please contact us.

11. How long we will keep your data

Once EUR confirms that your data has been correctly received, we will delete it from our systems and stop processing it for the aforementioned purpose.

If you consent to 6.ii, we will keep the responses for the Project duration plus 10 years.

12. Your rights

You have the right to request that we:

- provide you with information as to whether we process your data and details relating to our processing, and with a copy of your personal data;
- rectify any inaccurate data we might have about you without undue delay;
- complete any incomplete information about you;
- under certain circumstances, erase your Personal Data without undue delay;
- under certain circumstances, be restricted from processing your data;
- furnish you with the Personal Data which you provided us within a structured, commonly used and machine-readable format when the processing is based on the consent or on the contract.

You can withdraw your consent at any time. Please, keep in mind that the withdrawal will not affect the lawfulness of processing based on consent before its withdrawal.

Requests for any of the above should be addressed by email to [Insert contact details]. Your request will be processed within 30 days of receipt. Please note, however, it may not be possible to facilitate all requests, for example, where EUR is required by law to collect and process certain personal data including that personal information that is required of any research participant.

It is your responsibility to let the Principal Investigator know if your contact details change.

You have a right to lodge a complaint with the Office of the Data Protection Supervisory Authority of your country.

Last updated

05/09/2025

Annex 1.6

Status: Planned. This annex will be added once produced.

Annex 1.7

Cookie Policy - KEEPCARING.EU

We want to explain to you what cookies (and similar tracking technologies) are, what types of cookies we use on the Website of the KEEPCARING Project and how you can change your cookie preferences at any time.
The Website is managed by two partners of the KEEPCARING Project:

- NUROMEDIA GMBH, established in Schaafenstrasse 25, KOLN 50676, Germany ["NURO"] and
- ECHALLIANCE COMPANY LIMITED BY GUARANTEE, established in 20 Harcourt Street Raheny, DUBLIN D02H364, Ireland ["ECHA"].

For more information on how we process your personal data, we invite you to read the Website's Privacy Policy.

WHAT ARE COOKIES?

Cookies and similar technologies such as pixels or tags (collectively "cookies") are small files or pieces of code that can collect information about users when they navigate a website or an application (mobile or web). Cookies can be stored on users' devices for a certain period of time, in order to facilitate or improve the browsing experience. Cookies can have various functions and durations, as explained below.

Categories of cookies

Strictly necessary cookies are essential cookies for the correct functioning of a platform, site or app. Generally, they include technical cookies that allow users to load and navigate between the pages of a site, use the basic functions of an app and navigate safely. These cookies are always active and do not require prior consent from users as they are essential tools to ensure a smooth and safe browsing experience.
Other categories of cookies include, among others, **functional cookies** (for example, those cookies used to improve the user's browsing experience, such as those that remember the preferred language or login data), **performance measurement cookies** (for example, to collect

information such as the number of users or session statistics) and **targeting cookies** (for example, to create user profiles and display personalized ads or content). Since all these cookies are not strictly necessary from a technical point of view, prior consent from users is required before these cookies are activated.

Duration of cookies

Cookies can have different durations. **"Session cookies"** are automatically deleted when the user closes the browser, while **"persistent cookies"** remain on the user's device until a pre-set date. Thanks to persistent cookies, a website can remember the actions and preferences of users (such as login data, default language, font size, additional display settings, etc.) so that they do not have to be specified another time when the user visits the website again. Persistent cookies also have a pre-set expiration date, after which they are automatically deleted from the user's device.

Firstparty or third-party cookies

Finally, a distinction can be made between **first-party cookies** and **third-party cookies.** First-party cookies are cookies set by the website owner themselves, while third-party cookies are set by other parties, such as an external service provider (for example, Google).

THE COOKIES WE USE ON OUR WEBSITE

In this section you can find more information about the cookies used by our webiste. You can always change your cookie preferences using the banner "Manage consent" available in the bottom right corner of every page of the website.

List of cookies

Strictly Necessary Cookies (Functional cookies)

These cookies are necessary for the website to function properly and cannot be switched off in our systems. They are usually only set in response to actions made by you which amount to a request for services, such as setting your privacy preferences, logging in or filling in forms.

Cookie	Supplier	Purpose	Retention
Multilanguage cookie	Polylang	Saves the detected browser language/ language set via language switcher	365 Days
Cookie Notice	Complianz	Saves the user's preferences regarding cookies usage along with the cookie banner state	365 Days

Statistics cookie

To analyze how users interact with our platform and to provide some specific features, we use Google Analytics, a service provided by Google Ireland Limited that allows us to collect and analyze data relating to different types of events (interactions with our products, app errors and malfunctions, etc.).
Since these cookies are not strictly necessary from a technical point of view, prior consent from users is required before these cookies are activated.
For more information about Google Analytics, please click here.

How to block cookies

By entering our platform, the user can choose to accept all cookies or reject them (except those strictly necessary) by closing the banner or selecting the "Deny" option.
You can change your cookie preferences at any time by clicking on the "Manage consent" button displayed on the bottom right corner of every Webpage. You can then adjust the available sliders to "On" or "Off", then click on "Save Preferences". You may need to refresh the page for the settings to take effect.
Alternatively, most web browsers allow you to change your cookie preferences through your browser settings. To find out more about cookies, including how to see what cookies have been set, you can visit www.aboutcookies.org.

This policy was last updated on 10/06/2025.

Annex 1.8

Information letter on the

Participation in the co-design event
"Co-design of the online Change Management Platform"

KEEPCARING -
Future Proofing Health and Care Systems Safeguarding Healthcare Professionals in Hospital Settings
Grant Agreement No. 101137244

HORIZON-HLTH-2023-CARE-04
Topic HORIZON-HLTH-2023-CARE-04-02 - Ensuring access to innovative, sustainable and high-quality healthcare

Introduction to the KEEPCARING project (www.keepcaring.eu)
The co-design event is part of a larger research project funded by the EU, KEEPCARING. The project addresses the stress and burnout among healthcare professionals in the European Union.
The KEEPCARING project was initiated to fundamentally improve the well-being of healthcare professionals across the European Union. The project seeks to co-create a comprehensive solution package specifically designed to reduce stress and enhance resilience in healthcare workers at every level—individuals, teams, and organizations. You can find the partners of the Project and have more information about it at https://keepcaring.eu/.

WHAT IS THE CO-DESIGN EVENT ABOUT?
As part of the KEEPCARING Project, this co-design event is the first step towards the creation of the KEEPCARING Change Management Platform (CMP), part of the project's solution package. The CMP will be a companion app for mobile devices presenting goals and mission, overview, innovative integrative solutions (active interaction with end-users, participative scenarios, assessment forms) and management approaches able to impact organizational models to support healthcare decision-makers in addressing stress and burnout among healthcare professionals.

For this co-design event "Consiglio Nazionale delle Ricerche ("CNR", "we", "us")" is the controller of the personal data that will be processed.

Before deciding whether you want to participate in the co-design event described, please, read this document carefully. Please ask all the questions you may have so you can be completely sure to understand all the proceedings of the co-design event including risks and benefits (see contact details section).

DURATION OF THE RESEARCH ACTIVITIES
The KEEPCARING Project activities run for 48 months, from 01/07/2024 to 30/06/2028.
The co-design event in which you will take part will last for a total of 2 hours

WHY WE NEED YOUR COLLABORATION
With your participation, you will provide a substantial contribution to associating end-user knowledge with the design and increasing the suitability between the mobile application and users' needs and requirements.

WHAT CAN YOU EXPECT?
If you choose to participate in this co-design event, you will take part in a live co-design session that will take place in Rome, on the 24th of February 2025 for a total duration of 2 hours.

Please note that the co-design event will be held in a hybrid setting. This means it will be possible to join the discussion through the Microsoft Teams platform.
During the event, we will ask you to express your opinion on a series of pre-defined questions. To collect and later analyze your answers we will use a tool called "Slido".

The data collected through the co-design event will be dealt with at the highest possible level of diligence and will only be shared with researchers involved in the KEEPCARING project, in particular with partners involved in the work package dedicated to the development of the CMP. In scientific publications and project reports, information will be presented in aggregated and anonymized form per stakeholder group or other characteristics.

There is no remuneration for your participation in the study.

YOU DECIDE WHETHER TO PARTICIPATE

Participation in this event is completely voluntary. You can stop at any time and would not need to provide any explanation.

WHAT DATA WILL WE ASK YOU TO PROVIDE?

We will collect, process, and store your personal data based on your consent (Art. 6 (1) (a) GDPR). In particular, we will process your:
-name and email contact information in case we need to get in touch with you regarding the co-design event results;
-gender;
-affiliations and stakeholder type;
-opinions and answers for the purpose of the co-design event;
-ip address, when you use Slido.

We will also collect your image and voice, since an audio-video recording of the event will be made. When the footage and/or photographs are generic and include multiple people and concern the activities carried out during the Event, the legal basis is the company's legitimate interest in documenting the Event and keeping record of the discussion. The photos will be published on social media networks and will be attached to the project's deliverables. You can object to the processing from the beginning and you will still be able to take part in the event.
For photographs and/or video recordings, which directly and explicitly portray the data subject in order to be published for promotional purposes on paper materials or electronic/digital channels (e.g. brochures, flyers, websites, social networks, etc.), the legal basis is the consent of the data subject. Consent is optional and, in case of refusal, the photos or videos cannot be taken and used.

If you decide to join the event via the Teams platform, you can simply keep your webcam off to avoid being video recorded.

At the end of the event, you will be asked to complete a questionnaire to prioritize the features and requirements identified during the co-design discussions.

We do not need your personal identifying information for the purpose of the co-design creation, therefore we won't associate your name and contact information with the data collected through the audio/video recording, the "Slido" tool and the conclusive questionnaire.

The data will be collected through the researcher's laptop. After anonymization and aggregation, it will be uploaded on the project's One drive, hosted by one of the Project's partners, Erasmus University of Rotterdam (EUR).

HOW LONG DO WE KEEP YOUR DATA?

Your anonymized data will be retained after completion of the research. We retain the data so that other researchers have the opportunity to verify that the research was conducted correctly.

Your name and contact details will be deleted within 1 year after completion of the research.

WHO CAN SEE YOUR DATA?
Partners of the Project access anonymized and aggregated data about opinions and answers on the co-design event. Only CNR will have access to the email addresses of participants who explicitly gave their consent.

WHERE IS YOUR DATA?
We store the data in the EU. However, we rely on our suppliers Microsoft and Cisco Systems (provider of Slido) which can have access to the data form outside the EU for the provision of some services.
In this case, the transfer occurs in accordance with the safeguards set out in Chapter V of the GDPR (adequacy decision or, in the absence, based on the Standard Contractual Clauses adopted by the EU Commission). If you wish to know more about these transfers please contact our DPO at dpo@cnr.it.

CONTACT DETAILS
In case of any issue or question about your participation in the co-design event or about your privacy rights, such as accessing, changing, deleting, or updating your data, please contact us:

Maria Chiara Caschera
mariachiara.caschera@cnr.it
CNR

Do you have a complaint or concerns about your privacy? Please email the Data Protection Officer at dpo@cnr.it.

DO YOU REGRET YOUR PARTICIPATION?
You may regret your participation. Even after participating, you can still stop. Please indicate this by contacting us. We will delete your data. Sometimes we need to keep your data so that, for example, the integrity of the study can be checked.

YOUR RIGHTS UNDER THE GDPR
You have the right to:

- obtain information as to whether we process your data and details relating to our processing;
- access and obtain a copy of your personal data;
- modify or correct any erroneous data;
- request that restrictions be placed on the processing of your data;
- request that we erase your data;
- request to transfer or receive a copy of your data, in accordance with the right of data portability.

Requests for any of the above should be addressed by email to the Principal Investigator at mariachiara.caschera@cnr.it (email of the principal investigator for CNR) and the Data Protection Officer at dpo@cnr.it. Your request will be processed within 30 days of receipt. Please note, however, it may not be possible to facilitate all requests, for example, where the CNR is required by law to collect and process certain personal data including the personal information that is required of any research participant.

It is your responsibility to let the Principal Investigator know if your contact details change.

In case there is reason to assume that the processing of your data violates data protection law or if your data protection rights have been otherwise infringed, you have the right to lodge a complaint with the supervisory authority of your country.

Annex 1.9

Status: Planned. This annex will be added once produced.

Annex 2.1

DATA SHARING AGREEMENT

for the research project

"**KEEPCARING**"

Purpose of this agreement: this agreement sets the terms and conditions for sharing personal data between Party A, Party B, Party C, Party D, E as joint data controllers

This Data Sharing Agreement shall be effective as of the date of the last-executed signature below ("Effective Date") is made by and between:

1. **University of Limerick, of Plassey, Limerick Ireland**, (" UL" or "Party A");
2. **NOVA University Lisbon, Portugal),** (" NOVA" or "Party B");
3. **University of Coimbra, Portugal,** ("UC" or "Party C")
4. **The Capital Region of Denmark (Region Hovedstaden), with address Kongens Vænge 2, 3400 Hillerød, Denmark ,Business registration no. 29190623** ("short name" or "Party D")
5. **Universitätsklinikum Hamburg-Eppendorf, Körperschaft des öffentlichen Rechts,** represented by the board of directors, Martinistraße 52, 20246 Hamburg, Germany, with its conducting department Klinik und Poliklinik für Allgemein-, Viszeral- und Thoraxchirurgie [Department of General, Visceral and Thoracic Surgery] ("UKE" or "Party E") under the direction of Prof. Dr. med. Felix Nickel ("Investigator")[1] and PD Dr. med. Anna Niessen (Co-Investigator)

individually referred to as a "**Party**" and collectively referred to as the "**Parties**".

BACKGROUND

(A) Party A, Party B, Party C, Party D, and Party E collaborate in the Horizon Europe-funded Project entitled KEEPCARING, together with other Partners;

(B) The Project is regulated by the Grant Agreement n. 101137244;

(C) The aim of the Project is to (re-)build wellbeing and resilience of healthcare workforce in EU hospitals by co-creating a multi-faceted non-digital, digital and AI-supported solution package to prevent burnout among (aspirant) healthcare professionals on the individual, team, and organisational level;

(D) Within the project, Work Package 2 (WP2) builds an evidence-based and intervention-oriented framework of the biopsychosocial mechanisms of stress and resilience of healthcare professionals. A triangulation design methodology will be employed to obtain different but complementary data to better understand resilience in healthcare professionals and how it affects their health and well-being;

(E) Under WP2, Party A, Party B, Party C, Party D, and Party E are to work collaboratively on research which will involve the sharing of Personal Data by a Party(ies), as applicable, for the [Prediction of resilience and burnout among hospital-based nursing and medical personnel] as described in Appendix 1(the "Study/Research").

(F) The Parties have agreed to share and process data including Personal Data as described in Appendix 2 for the purposes of the Study/Research (the "Shared Personal Data").

(G) Party A, Party B, Party C, Party D, and Party E have jointly determined the purposes of the Processing (as defined below) for the Study/Research as specified in Appendix 1("Agreed Purpose").

(H) The Parties wish to set out the principles and procedures that the Parties shall adhere to in relation to Shared Personal Data being shared for the Agreed Purpose.

(I) The Parties wish to enter into this Agreement to comply with the requirements of the current legal

framework in relation to Data Processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Therefore, the Parties agree as follows:

Data Controller	means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
Data Processor	means any person (other than an employee of the data controller) who processes the data on behalf of and under the instruction of the Data Controller.
Data Protection Laws	means all relevant national and European legislation and regulations relating to the protection of personal data including (without limitation) the General Data Protection Regulation and all other regulatory guidelines (whether statutory or non-statutory) or codes of practice or guidance issued by the European Data Protection Board (the "EDPB") relating to the processing of personal data or privacy or any amendments and re-enactments thereof.
	Data Discloser means the Party transferring the Personal Data to the Data Receiver. Either Party may be a Data Discloser.
	Data Receiver means the Party receiving the Personal Data from the Data Discloser. Either Party may be a Data Receiver.
	Data Subject means an individual, whether a patient or not, who participates in the Study whose data (including personal data) is being shared by the Parties for the Agreed Purpose.
Delete	means removing all electronically held Personal Data in such a way that it can never be retrieved from the device on which it is stored/ held, as well as securely disposing of non-electronic archives (if they exist).
GDPR	means the General Data Protection Regulation (Regulation (EU) 2016/679).
HRR	means the Data Protection Act 2018, (Section 36)2) (Health Research) Regulations 2018.
Joint Controller	shall mean two or more Data Controllers jointly determining the purposes and means of processing as defined in Article 26 of GDPR.
Loss	includes any claim, suit, proceeding, judgement, loss, liability, cost, expense, fee, penalty or fine;
Personal Data	shall mean any personal data (as defined in the GDPR) Processed by a Party in connection with this Agreement, and for the purposes of this Agreement includes the special categories of sensitive personal data as listed in Article 9(1) of GDPR.
Processing	shall mean any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination,

	restriction, erasure or destruction (and Process and Processed should be construed accordingly).
Pseudonymisation	shall have the meaning given to that term in Article 4 of the GDPR.
Shared Personal Data	means the Personal Data to be shared and processed between the Parties. Shared Personal Data shall be confined to that listed in Appendix 2. Each data set of Shared Personal Data to be listed separately in Appendix 2, as applicable.

1. JOINT CONTROLLER OBLIGATIONS

1.1. The Parties acknowledge that a Party (as the Data Discloser), will as necessary disclose to the other Party (as the Data Recipient) Shared Personal Data collected by the Data Discloser for the Agreed Purpose.

1.2. Each party shall comply with all the obligations imposed on a Data Controller under the Data Protection Laws in the performance of its obligations under this Agreement and any other agreement between the Parties which pertains to Shared Personal Data ("Relevant Agreements"), and any material breach of the Data Protection Laws in respect of a Relevant Agreement by one Party shall, if not remedied within 30 days of written notice from the other Party, give grounds to the other Party to terminate this Agreement with immediate effect.

1.3. Each Party will Process that Shared Personal Data only for the purpose of carrying out the Agreed Purpose.

1.4. Each Party will take such technical and organisational measures as may be appropriate to ensure the security of that Shared Personal Data (including by way of example and without limitation, the Pseudonymisation and encryption of Shared Personal Data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services and the ability to restore the availability and access to Shared Personal Data in a timely manner in the event of a physical or technical incident). Without prejudice to the generality of the foregoing, each Party will keep that Shared Personal Data secure from any unauthorised or accidental use, access, disclosure, damage, loss or destruction.

1.5. Each Party will ensure that access to that Shared Personal Data is limited to those of its employees, staff, officers, researchers and agents who need access to the Shared Personal Data for the Agreed Purpose and will take reasonable steps to ensure the reliability of such persons which shall include ensuring that such persons understand the confidential nature of the Shared Personal Data, have received appropriate training in data protection prior to their use of the Personal Data and have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. This duty of confidentiality shall remain in effect even after the termination of the agreement.

1.6. Each Party will not authorise any third party or sub-contractor to Process any Shared Personal Data without (i) first notifying each of the other parties and (2) entering into a contract with that third party or sub-contractor on terms which are substantially the same as the terms set out in this Agreement The processing of Shared Personal Data under such contract shall cease upon the earliest occurrence of (a) termination or expiry of this Agreement, (b) the end of the Study or (c) the sharing of Personal Data between the Parties no longer being required for the purposes of the Project.

1.7. Each Party will give the other Party such information and assistance as it reasonably requires in order to enable the other Party to meet its obligations to data subjects concerning the Shared Personal Data, in particular, but without limitation, complying with Data Subjects' requests for access to, information about, and the rectification of, their Personal Data.

1.8. Unless agreed otherwise between the Parties, the Party which is responsible for obtaining the patient consent for the Study/Research shall be appointed as single point of contact (SPoC) for Data Subjects. The SPoC shall be detailed within Appendix 2 of this Agreement.

1.9. The SPoC is responsible for maintaining a record of individual requests for information, the decisions made and any information that was exchanged. Records must include copies of the request for information, details of the data accessed and shared and where relevant, notes of any meeting, correspondence or phone calls relating to the request.

1.10. Each Party will notify the other Party immediately should it receive any request or enquiry from any Data Subject in relation to the Shared Personal Data being Processed for the purpose of the Study, give the other Party such assistance in dealing with that request or enquiry as it may reasonably request; and not disclose or release Shared Personal Data without first consulting with the other Party wherever possible.

1.11. Each Party will notify the other Party without delay and, in any event, no later than 48 hours after becoming aware of any actual or suspected breach of security which involves the Shared Personal Data or breach of this Clause 1.

1.12. In respect of any Shared Personal Data breach, each Party, without undue delay and, in any event, no later than 48 hours after becoming aware of the Shared Personal Data breach (in accordance with applicable law) will notify the other Party of the Personal Data breach and provide the other Party with such details as the other Party reasonably requires regarding the nature of the Shared Personal Data breach (including the categories and approximate numbers of Data Subjects and protected data records concerned or likely to be concerned), any investigations into such Shared Personal Data breach, the likely consequences of the Shared Personal Data breach and any measures taken, or recommended, to address the Shared Personal Data breach, including to mitigate its possible adverse effects.

1.13. At the other Party's written request without delay (in accordance with the applicable law), each Party will either securely Delete or securely return to the other Party all the Shared Personal Data that the other Party has shared with it in such form as it requests after the earlier of:

1.13.1. the expiry or termination of this Agreement;

1.13.2. the end of the Study; or

1.13.3. the sharing of the Shared Personal Data in question no longer being required for the purposes of the Study; and

securely Delete existing copies (unless storage of any data is required by applicable law and, if so, it will inform the other Party of any such requirement).

1.14. Each Party will promptly (and in any event within two Business Days) inform the other Party if it receives a complaint or request relating to either Party's obligations under the Data Protection Laws relevant to this Agreement, including any compensation claim from a data subject or any notice, investigation or other action from any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering any Data Protection Laws and provide the other Party with full details of such complaint or request; and

1.15. Each party undertakes not to disclose the Shared Personal Data to third parties who are not involved in the Project, unless the other Parties authorise such disclosure in writing. Each Party will not transfer the Shared Personal Data outside the European Economic Area without first informing the other parties and confirming that the proposed transfer is compliant with Chapter V of GDPR).

1.16. Each Party will ensure that the sharing of responsibilities between all Parties reflects the Joint Controller Matrix in Appendix 3 of this Agreement.

2. **AUDIT**

Each Party will allow the other Party at all reasonable times agreed in advance by each party, and on reasonable written notice to inspect and review the steps being taken by it to comply with Clause 1 above, and will give the other Party any assistance which it reasonably requires with that inspection and review. The monitoring, visits and/or audits take place in accordance with applicable data protection laws.

3. DATA PROTECTION

The Parties must comply with all Data Protection Laws that apply to them in relation to Shared Personal Data processed in connection with the Study and the performance of this Agreement. The further handling of personal data, in particular patient data, is subject to appendix 3 to this Agreement

4. TERMINATION

4.1 Subject to clause 4.2 either Party may terminate this Agreement upon giving one month's prior written notice to the other.

4.2 The provisions in this Agreement will continue in full force and effect for so long as a Party is a Data Controller or shares any Personal Data with the other Party, notwithstanding the expiry or termination of this Agreement or the completion of the Study/Research.

4.3 Without prejudice to any termination rights in this Agreement, if any Party is in breach of its obligations under Clause 1, the other Party may suspend any sharing of Shared Personal Data for the purposes of the Study/Research until the breach is remedied.

5. DATA RETENTION

5.1 The Parties shall not retain or process Shared Personal Data for longer than is necessary to carry out the Agreed Purposes.

5.2 The data for this Study/Research shall be held for 5 years after the completion of the Study/Research to assist in the academic publication process for the dissemination of findings. ASSIGNMENT

Neither Party shall assign, sub-licence, delegate or otherwise transfer all or any of its rights or obligations under this Agreement, without the prior written consent of the other Party.

6. Liability

6.1. The liability provisions as set out in Clause 5 of the Consortium Agreement shall apply *mutatis mutandis* this Agreement.

6.2 However, notwithstanding Clause 5 of the Consortium Agreement Art. 82 GDPR shall remain unaffected. Each party shall be liable to the other parties for any Losses suffered or incurred by the other parties arising out of or in connection with all claims, proceedings or actions brought by a competent public authority or a data subject with respect to the processing of personal data by the other party

7. GENERAL

7.1 Each of the provisions of this Agreement is separate and severable and enforceable accordingly. If at any time any of the provisions is held to be void or unenforceable, the validity or enforceability of the remaining provisions shall not be affected. If any provision is held to be void or unenforceable, the Parties agree to substitute any such provision with a valid enforceable provision which achieves to the greatest extent possible the economic, legal and commercial objectives of the invalid or unenforceable provision.

7.2 This Agreement represents the entire agreement between the Parties with respect to the subject matter therein and supersede all prior representations, agreements, arrangements and undertakings with respect thereto whether written or oral. This Agreement may only be amended in writing signed by duly authorised representatives of the Parties.

7.3 Neither this Agreement nor any subsequent discussions between the Parties shall create any obligations other than those expressly stated herein. Nothing in this Agreement shall oblige either Party to enter into any further agreement with the other in relation to the subject matter of this Agreement.

7.4 All notices given by a Party to the other pursuant to this Agreement shall be in writing and may be delivered by email, including request of read receipt, or pre-paid post, registered courier, by hand to the address at the beginning of this Agreement.

Notice to Party A shall be sent to:
Stephen Gallagher
Department of Psychology, University of Limerick, Ireland)
stephen.gallagher@ul.ie

Notice to Party B shall be sent to:
Luís Silva
Physics Department, LIBPhys-UNL, Universidade NOVA de Lisboa, *Campus* de Caparica | 2829-516 Caparica | Portugal
lmd.silva@fct.unl.pt with a copy to dpo@unl.pt

Notice to Party C shall be sent to:
Diana Ribeiro da Silva
Faculty of Psychology and Education Sciences, University of Coimbra
Rua do Colégio Novo, 3001-802 Coimbra, Portugal
diana.rs@fpce.uc.pt

Notice to Party D shall be sent to:
Jeanett Strandbygaard
Capital Region of Denmark
jeanett.strandbygaard@regionh.dk

Notice to Party E shall be sent to:
Prof. Dr. med. Felix Nickel
Universitätsklinikum Hamburg-Eppendorf
f.nickel@uke.de

Any such notice, if so given, shall be deemed to have been served:

(a) if sent by hand, when delivered;
(b) if sent by post or courier, ten business days after posting.
(c) If sent by email, upon read receipt notification

7.5 This Agreement may be executed in any number of counterparts all of which taken together shall constitute one single agreement between the Parties. Transmission of an executed counterpart of this Agreement by e-mail (in PDF, JPEG or other agreed format) shall take effect as delivery of an executed counterpart of this Agreement. The Parties acknowledge and agree that this Agreement may be executed by electronic signature, which shall be considered as an original signature for all purposes and shall have the same force and effect as an original signature. Without limitation, "electronic signature" shall include emailed versions of an original signature or electronically scanned and transmitted versions (e.g., via pdf) of an original signature.

7.6 This Agreement shall be governed by and construed in accordance with the laws of Belgium and the Parties submit to the exclusive jurisdiction of the Irish courts as regards any claim or matter arising under this Agreement, provided that it does not conflict with national legislation or EU law.

7.7 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of Brussels .

The Parties hereto have caused this Agreement to be executed the day and year herein first appearing by their duly authorised representatives

APPENDIX 1
Description of the Study

The study aims to assess and predict levels of resilience and burnout among hospital-based nursing and medical personnel and how do factors like work setting factors influence them. This information will help us understand how burnout happens, what factors make it happen, and what the health services can do about it.

Study design: a cross-sectional online survey using socio-demographics, job characteristics and validated measures of resilience, work stressors, leadership styles and burnout.

The survey is the main part of the study, but we will have a sub study that will allow those taking the survey to take part in either a qualitative (face-to-face interview) or a biosignal monitoring study). For the qualitative part it will be one to one semi structured interviews done on MS Teams, while the biosignal study participants will wear a hexoskin vest **(example here** https://www.mindtecstore.com/Hexoskin-Smart-Shirt-Women) at either University Amsterdam Medical Centers, Netherlands, The Capital Region of Denmark, Denmark, or Universitätsklinikum Hamburg-Eppendorf, Germany

APPENDIX 2[2]

TABLE – SHARED PERSONAL DATA	
The subject matter of the Processing	To assess and predict levels of resilience and burnout among hospital-based nursing and medical personnel. This information will help us understand how resilience and burnout influenced in the hospital context and what the health services can do about it.
The nature and purpose of the Processing	For the purposes of the study, the following processing operations will take place • Collection of data • Organisation of data • Adaptation of data • Alteration of data • Anonymisation of data • Storage of data • Consultation of data • Erasure of data • Destruction of data
The type of Personal Data being Processed	Answers to survey questions including • name • age • marital status, • gender, ethnicity, • country, • job role, • Training and speciality, • duration of employment Hexoskin wearable vest - heart rate
The categories of data subjects	• Research subject
Party responsible for providing information under art 13 and 14 i.e. data protection notice	Document the SPOC UL(Stephen Gallagher- for survey/interviews) and Luís Silva (Hexoskin study) Physics Department, LIBPhys-UNL, Universidade NOVA de Lisboa

[2] Table to be replicated and completed for each data set of Shared Data.

APPENDIX 3

Joint Controllers Matrix

Data protection obligation	Responsible party
Provide information on the processing of personal data to data subjects in accordance with articles 13 and 14 GDPR.	UL(Stephen Gallagher- for survey/interviews) and Luís Silva (Hexoskin study) Physics Department, LIBPhys-UNL, Universidade NOVA de Lisboa
Obtaining informed consent for the processing of personal data or establish another legal basis for the processing of personal data.	UL(Stephen Gallagher- for survey/interviews) and Luís Silva (Hexoskin study) Physics Department, LIBPhys-UNL, Universidade NOVA de Lisboa
Safeguarding that the data subjects can exercise their rights under the GDPR	All parties. Processes and procedures shall be laid down to enable the exercise of data subjects' rights
Safeguarding the security of personal data in accordance with article 32 GDPR and in accordance with other arrangements in this Agreement.	All parties. Processes and procedures shall be laid down to enable the exercise of data subjects' rights
Comply with data breach obligations (articles 33 and 34 GDPR).	If any party becomes aware of a personal data breach in connection with this Agreement, that party shall promptly notify and, in any event, no later than 48 hours after becoming aware of the Shared Personal Data breach_the other Parties. Parties will fully cooperate with each other in order to fulfil the (statutory) notification obligations timely.
Safeguarding that employees who have access to personal data are instructed by a binding agreement or binding instruction(s) to process the personal data in conformity with the instructions of the controllers, including the duty of confidentiality.	All parties
Safeguarding that engaged (sub) processors who have access to personal data are instructed by a binding agreement (data processor agreement) to process the personal data in accordance with the requirements stated in article 28 of the GDPR.	All parties
Safeguarding that the transfer of personal data takes place in accordance with the GDPR.	All parties
Safeguarding the compliance with the requirements regarding retention periods, destruction, return and/or migration of personal data.	All parties provided that these requirements are made known to each other.
Safeguarding that a data protection impact assessment is conducted prior to the collection, including obtaining and further processing of personal data (Article 35 GDPR).	All parties
Cooperation with and audits by the supervisory authorities.	All parties
Anonymisation of data set and transfer to open access repository.	Parties A and B

Annex 2.2

Status: Planned. This annex will be added once produced.

Annex 2.3

KEEPCARING – WORKPACKAGE 3
STUDIES B, C and D
JOINT CONTROLLERSHIP AGREEMENT

BETWEEN:

Stichting Amsterdam UMC, having its principal place of business at De Boelelaan 1117, 1081 HV Amsterdam, the Netherlands, hereby represented by its fully owned subsidiary AMC Medical Research BV, lawfully represented in this matter by J.J. Brand, CFO of AMC Medical Research BV, the Coordinator ("AUMC");

Universitätsklinikum Hamburg-Eppendorf, Körperschaft des öffentlichen Rechts, located at Martinistraße 52, D-20246 Hamburg, Germany, duly represented by the board of directors, with its conducting department Klinik und Poliklinik für Allgemein, Viszeral- und Thoraxchirurgie

and

Stitching Rigshospitalet, having its principal place of business at Blegdamsvej 9, 2100 Copenhagen, Denmark, CVR-no: 29190623, hereby represented by its fully owned subsidiary Department of Thoracic Surgery, Anesthesiology and Intensive care, the Heart Center, RIGS and Department of Gynecology, Fertility and Obstetrics, Juliane Marie Centre, RIGS, lawfully represented in this matter by PRIVACY, the Capital Region of Denmark, the Coordinator ("RIGS").

hereinafter collectively referred to as the "Parties" and individually referred to as a "Party",

Whereas:

1. The Parties collaborate, together with other partners, on the Horizon Europe-funded Project entitled KEEPCARING - "Future Proofing Health- and Care Systems

Safeguarding Health Care Workers in Hospital Settings", further referred as "the Project";

2. The Project number is 101137244;
3. Healthcare professionals working in hospitals and those in training to embark on hospital careers experience high levels of stress, especially in the surgical pathways. While interventions to improve wellbeing and resilience exist, not much is known about the right (combination of) intervention(s) for this specific setting;
4. KEEPCARING aims to (re-)build wellbeing and resilience of healthcare workforce in EU hospitals by co-creating a multi-faceted non-digital, digital and AI-supported solution package to prevent burnout among (aspirant) healthcare professionals on the individual, team, and organisational level;
5. KEEPCARING has a multi-sector and interdisciplinary consortium that will (1) study stress and stressors experienced by (aspiring) health care providers in their specific setting, (2) evaluate digital and non-digital solutions to reduce stress at an individual and team level, (3) study job crafting among (aspiring) health professionals as a way to reduce stress, and (4) finally, develop a change management platform that, using explainable AI, helps hospital managers as well as surgical caregivers to choose the solutions that match their context;
6. The Parties, collaborating in "*Work Package 3 - Resilience Robustness 2. Solutions and interventions to reduce job stress across clinical settings*" have jointly defined three study protocols aimed at evaluating the effectiveness of digital solutions at reducing stress at individual and team level;
7. The Studies are identified as follows:
8. "Study B" - **Deep relaxation using Virtual Reality Therapy before surgery**;
9. Objectives: Determine (primary objective) whether deep relaxation using VR (Healthy Mind solution) before working in the OR is an effective (T3.2) and (secondary objective) cost-effective (T3.6) intervention to mitigate stress and help promote resilience, in comparison to a low-stimulus time out situation before working in the OR, as measured both within person and between groups;
10. "Study C" - **Evaluating Healthcare Professionals' Satisfaction and Stress Mitigation Using Virtual Reality Intervention in Surgical Ward: a multination feasibility study;**

11. Objectives: First, test a newly developed nature based VR environment that is able to adjust to real-time physiological parameters indicative for stress such as heart rate and heart rate variability. Next, assess user satisfaction among working staff involved in active patient care at the surgical wards with the ultimate goal of mitigating stress and promoting resilience. Additionally, study the perceived stress levels before and after the VR intervention;
12. "Study D" - **Longer term resilience: Team debriefing after surgery**;
13. Objectives: Examine whether teams who participate in ORBB (Operation Room Black Box) augmented debriefings feel equally psychological safe as teams who get non-video assisted team debriefing;
14. The Parties will be involved in each of the three mentioned Studies (collectively, "the Studies"), with different roles. The specific roles are identified below, in article 3;
15. In this context, the Parties collect, store, and share some personal data as defined by art. 4 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("General Data Protection Regulation' or "GDPR");
16. Since the Parties jointly determine the purposes of the Data Processing Operations and the means used therein, they are joint controllers within the meaning of Article 26 of the GDPR and they must transparently determine, through an internal agreement, their respective responsibilities regarding the obligations stemming from the personal data processing legislation.

Now, therefore, the Parties have agreed as follows:

Art. 1 Definitions

1.1 The terms controller, joint controllers, data processor, processing, data subjects, data breach used in this agreement have the meaning indicated in the GDPR.

Art. 2 Scope of the agreement and personal data processing

2.1 This agreement is designed to enable the Parties to comply with the obligations of the GDPR related to the processing activities carried out in Work Package 3 ("WP3"), for the purposes and with the means jointly determined as Joint controllers.
2.2 Joint controllership exists with respect to the data collected and processed by the Parties within the scope of the Project and in particular in the context of the Studies.

Art. 3 Roles, activities, legal bases and categories of data
3.1 AUMC is the principal investigator in studies B and C, while UKE and RIGS take part in these studies as Research associates. RIGS and AUMC are the principal investigators in study D, while UKE takes part in this study as Research associates.
3.2 In particular, for the purpose of collecting data, information and opinions through the execution of Study B, C and D, the Parties will collect and process the personal data listed in the following tables. In the case of studies B and C, personal data will belong to health care professionals that voluntarily decide to take part in one or both the studies. In the case of Study D, personal data will belong to patients undergoing surgery and health care professionals belonging to the Operating Room team.

Table 1. Data processed in Study B

Data categories	Examples of Data items	Data subjects
Identification data	Name, Surname	Health care professionals employed in the operating rooms of the three Parties' University Hospitals or other participating hospitals
Contact data	Email	
Demographic data	Sex, Age	
Professional data	Profession, Hospital, Specialty, Country, Work experience, Workhours per workweek	
Usage data	Type of VR environment chosen and VR environment changes in correlation with measured heart rate	

Non-invasive biomarkers *Health data under Art. 9 GDPR. Measured and calculated by POLAR H1*	Heart rate, Heart rate variability	
Prescription of medications *Health data under Art. 9 GDPR*	Medication use for symptoms of anxiety, stress and-or depression	
Opinions *May constitute Health data under Art. 9 GDPR*	Questionnaire answers related to several relevant topics, among which: Perceived stress level, Satisfaction with the intervention	
Habits	Smoking habits, sleep patterns	
Analysed data *Health data under Art. 9 GDPR*	Correlation between perceived stress and non-invasive biomarkers, Association between baseline characteristics (e.g. demographic data) and stress	

*Table 2. Data processed in Study C **

Data categories	Data items	Data subjects
Identification data	Name, Surname	
Contact data	Email	

Demographic data	Sex, Age	Health care professionals employed in the surgical wards of the three Parties' University Hospitals or other participating hospitals
Professional data	Profession, Hospital, Specialty, Country, Work experience, Workhours per workweek	
Usage data	Type of VR environment chosen and VR environment changes	
Opinions	Questionnaire answers related to a number of relevant topics, among which: Perceived stress before and after the VR intervention, Satisfaction with the intervention, User comfort (CyberSickness in Virtual Reality Questionnaire (CSQ-VR)), comfort with perceived complexity, Perceived disadvantages, Personal emotion, Social influence, Perceived advantages, Optional follow up interview with 5 participants; Audio recordings of the interviews (discarded after transcription)	
Analysed data	Statistical analysis of the collected data points, Association between baseline characteristics (e.g. demographic data) and user satisfaction	

Table 3. Data processed in Study D

Data categories	Data items	Data subjects
Observational data through the ORBB	Audiovisual data (blurred) and video data from endoscope	Patients undergoing surgery
Electronic health record data	Data imported from the EHRD in the ORBB platform, including type of surgery, length of surgery, wheels in and wheels out, HL7 data	
Identification data	Name, Surname	Health care professionals operating in Operation Room of the three Parties' University Hospitals
Contact data	Email	
Observational data of the team debriefing (non-ORBB intervention in UKE)	Detailed field notes documenting, among others, team members' engagement levels, communication styles, decision-making processes, conflict resolution approaches, and the interpersonal nuances that emerge during collaborative discussions	
Observational data through the ORBB (AUMC and RIGS)	Detailed field notes, Real-time video and audio recordings of surgical procedures performed by the OR team.	

Opinions	Data collected via self-reported measurements through questionnaires and qualitative interviews, Audio recordings of the interviews	

3.3 The Parties agree that data subjects participating in the Studies will take part in a series of activities designed as part of the KEEPCARING project. Several data collection methods (e.g., monitoring of non-invasive biomarkers, interviews, questionnaires, audio/video capturing) will be used to engage with participants in the Studies.
The Parties have agreed on three *ad hoc* Research Protocol, Privacy Notices and Informed consent modules. These documents provide more detailed information about data collection and data processing activities.
3.4 Each of the Parties is responsible for the collection and the processing of personal data in each respective site. Each Party will handle the information received with the highest possible level of diligence and will share it with the other Parties only in pseudonymised form. For this, a list of identification codes will be created, and participants will be linked to a code. Participants can be identified by their ID number. The participation identification log will be kept separate from the participant data and will be safeguarded by the local principal investigator. For the participating centres, a separate site-specific subject identification log will be kept at each study site.
Data will be securely stored in a restricted-access account on Castor EDC, accessible only to the Parties. AUMC will be the account holder and administrator for Studies B and C, while AUMC and RIGS will manage the account for Study D. Each participating centre will receive their own login credentials, granting access only to their own data, while the coordinating centre will have access to all data.
3.5 Only anonymous data will be shared with other KEEPCARING consortium partners for the purposes of the Project. In scientific publications and Project reports, information will be presented in anonymous form, ensuring that individual responses cannot be linked back to any specific participant.
3.6 The legal basis for the processing of personal data in the context of the Studies is the data subjects' consent (Art. 6 (1) (a) GDPR) and, where special categories of personal data

are collected, the parties will rely on the exception granted by art. 9(2)(a), i.e. the explicit consent of the data subject.

Art. 4 Lawfulness of processing and data subjects' rights

4.1. Each of the Parties undertakes to process the data in compliance with the GDPR and any other applicable national and supranational privacy and data protection laws. In particular, they must adopt all the necessary technical and organisational measures to ensure the exercise of data subjects' rights and that they answer to their requests in a timely manner.

4.2. The Parties are responsible for ensuring that there is a valid consent for processing the data and they must be able to demonstrate this.

4.3 The Parties will not collect more personal data than is strictly necessary for the purpose in question. The Parties will only process Personal Data for the purpose for which Personal Data was collected, unless the Parties agree, after consultation, that Personal Data may also be used for purposes that are sufficiently connected to the purpose for which it was originally collected (art. 6 (4) GDPR).

Art. 5 Data subjects' rights

5.1. Right to be informed. The Parties will make sure that data subjects receive the required information (as described in article 13 and 14 of the GDPR) when personal data is collected. They will make sure that data subjects know the name and the contact details of the joint controllers, the purposes of data processing, the legal basis for processing and be well informed about the data recipients and the retention period. All this information will be explained in a concise, transparent, intelligible and easily accessible form with clear and simple language. To this end, the Parties have agreed on the text of the Privacy Notice that will be provided to the data subjects participating in the Studies at the time of their recruitment for the Project.

5.2. Right of access. The Parties undertake to respect and guarantee the right of access of the data subjects pursuant to Article 15 of the GDPR. The Parties acknowledge that the obligation to comply with a data subject's request lies with the Party to which the request was submitted, unless the data in question can be attributed to a specific Controller. In such instances, that controller assumes this responsibility. Should it become necessary, the Parties will provide each other promptly with any reasonable assistance necessary to ensure

requests are addressed and to respond to any other questions or complaints raised by Data Subjects. In any event such assistance will be provided within 5 working days of a request for assistance.

5.3. Regardless of the internal arrangements, the Parties acknowledge that data subjects may exercise their rights under Articles 15 to 22 of the GDPR with regard to and against any of the Parties (Art. 26 (3) GDPR).

5.4. Right to erasure of data. If personal data must be deleted, the Parties shall inform each other in advance. A Party may object to the deletion for justified reasons, for example if it is subject to a legal obligation to retain the data.

5.5. Rectification of information. If any party becomes aware of errors or irregularities in personal data, it must inform the other parties within 5 working days and promptly rectify them.

5.6. The contact point to be contacted for the exercise of rights are:

AUMC: privacy@amsterdamumc.nl

UKE: dsb@uke.de

RIGS: forskningsjura.rigshospitalet@regionh.dk

5.7. Each party shall inform the others of any change regarding the indicated point of contact.

Art. 6 Making the essential content of the agreement available to the data subjects

The Parties undertake to make available to the data subjects the essential content of this joint controllership agreement, at the data subjects' demand.

Art. 7 Security of processing and evidence of compliance with the GDPR

7.1 Each Party will be responsible to implement appropriate technical and organisational measures to ensure and demonstrate that the processing is in compliance with the GDPR, taking into account the nature, scope, context and purposes of the processing involved, as well as the risks of varying degrees of likelihood and severity for the rights and freedoms of natural persons. The measures shall be reviewed and updated as necessary.

7.2 The Parties' measures shall include, where proportionate to the processing activities, the implementation of appropriate data protection policies.

7.3 The Parties shall be responsible for compliance with the data protection by design and data protection by default rule of Article 25 of the GDPR.
7.4 The Parties agree to use as a common Platform to gather, store and share pseudonymised data under this Agreement. The Platform is hosted by Ciwit B.V. and is called Castor EDC.

Art. 8. Use of data processors and sub-processors
8.1 The Parties are entitled to use processors and/or any sub-processors in connection with the joint processing operation.
8.2 In the event of use of processors and/or sub-processors, the Parties shall be responsible for complying with the requirements of Article 28 of the GDPR. Accordingly, inter alia:

1. use only processors that can provide the necessary guarantees that they implement appropriate technical and organisational measures in such a way as to ensure that processing complies with the requirements of the GDPR and safeguards the rights of the data subject;
2. ensure that a valid data processing agreement is in place between the Party and the processor; and
3. ensure that there is a valid sub-processor agreement between the processor and any sub processor.

8.3. The Parties may have Personal Data processed by other persons or organisations outside the European Economic Area, provided that the applicable laws and regulations regarding the Processing of Personal Data are observed.

Art. 9. Records of processing activities
9.1 Each Party is independently responsible for complying with the requirements of Article 30 of the GDPR on records of processing activities. Each Party shall report the processing activities carried out jointly and covered by this agreement in their own record of the processing activities.

Art. 10. Notification of personal data breaches to the supervisory authority

10.1 Each Party is and remains independently responsible for reporting any data breaches that take place under its responsibility to the Supervisory Authority and/or the data subjects, in accordance with Articles 33 and 34 of the GDPR.
10.2 Upon becoming aware of such a breach, a party must immediately inform all other parties within 24 hours, providing all relevant information about the breach necessary to make the notification. The notification must contain at least the following information:

- the nature of the personal data breach
- the categories and approximate number of the data subjects concerned
- the categories and approximate number of personal data records concerned
- the contact from which to obtain more information
- the description of the likely consequences of the breach
- the actions implemented or planned to be implemented to remedy the breach, and if applicable, a description of measures taken to mitigate any possible adverse effects.

10.3 The Parties will keep each other informed about the developments concerning the breach.
10.4 The Party where the breach occurred will bear any costs incurred for resolving the Breach, and for preventing any breaches in the future. The Parties may confer about a possible division of these costs if it concerns a solution that is in the interest of all the Parties.
10.5 The Parties are each responsible for keeping a data breach register.

Art. 11 Data protection impact assessment
11.1 The Parties shall be responsible for compliance with the requirement of Article 35 of the GDPR on data protection impact assessments ("DPIA").

Art. 12 Complaints
12.1 The Parties shall each be responsible for handling any complaints from data subjects, if the complaints relate to a breach of the provisions of the GDPR, for which the Party is responsible under this arrangement.
12.2 If one of the Parties receives a complaint, which should rightly be dealt with by the other Party, the complaint shall be forwarded to that Party as soon as possible.

12.3 If one of the Parties receives a complaint, part of which should rightly be dealt with by the other Party, that part shall be forwarded to the Party for reply as soon as possible.
12.4 The data subject shall be informed of the essential content of this arrangement when one Party forwards a complaint or part thereof to the other Party.

Art.13 Data Retention
The Parties agree that the data collected under this Agreement will be securely retained for as long as required by applicable laws and regulations, in accordance with the Research Protocol.

Art. 14 Secrecy and confidentiality
14.1 All Personal Data is classified as confidential information and will be treated as such. The Parties will also impose this duty of confidentiality on all persons or legal entities that they engage, including but not limited to Employees, Processors, Third Parties and other Recipients of Personal Data.
14.2 The Parties will maintain the confidentiality of all Personal Data and will not disclose it in any way whatsoever either internally or externally, except insofar as:
(i) the disclosure and/or provision of the Personal Data is necessary in the context of implementing the Grant Agreement or this Agreement;
(ii) a mandatory statutory provision or court order handed down by a competent court or order from any other governmental body having authority over the Parties obliges the Parties to disclose, provide and/or transfer this Personal Data. If this is the case, the Parties will first notify the other Parties in the process; or
(iii) disclosure and/or provision of this Personal Data is done with the prior Written permission of the other Parties.

Art.15 Final provisions
15.1 This arrangement shall enter into force upon signature by all Parties hereto.
15.2 The arrangement shall remain in force for as long as the data concerned are processed or until it is replaced by a new arrangement laying down the division of responsibilities in relation to the processing. Obligations ensuing from this Agreement that are, by their nature,

intended to continue after termination of this Agreement will continue after this Agreement is terminated.

15.3 Any changes to this agreement must be made in writing and agreed between the Parties.

15.4 If one or more provisions of this Agreement should prove to be legally void, the rest of this Agreement will remain in force. The Parties will then confer on the provisions that are not legally valid, with a view to making an alternative arrangement that is legally valid and, as far as possible, corresponds to the purport of the provision being replaced.

15.5 A Party that imputably fails to comply with any of its obligations under the GDPR or this Agreement, and as a result of which the other Parties are held accountable for damages, costs or interest by a Third Party, will indemnify the other Parties in full against the claims of this Third Party, unless the Party proves that the incident was caused by intent or gross negligence on the part of the other Party or Parties.

15.6 The obligations arising from this Agreement will also apply to those who process personal data under the Parties' authority, such as its employees and processors engaged.

Place and date

AUMC

UKE

RIGS

Annex 2.4

Study E: Data Protection and Management Framework

1. Introduction and Purpose

This document outlines the agreed-upon data protection framework for Study E. Its purpose is to ensure compliance with the General Data Protection Regulation (GDPR) and to protect the rights and freedoms of all research participants. This framework supersedes any previous discussions regarding a Joint Controllership Agreement (JCA), establishing a consent-based model for data sharing and processing. This approach has been chosen to provide greater administrative flexibility, particularly in light of the fact that additional hospitals are likely to be involved as the study progresses.

2. Overarching Principles

- **Legal Basis:** The primary legal basis for the sharing of personal data between participating institutions and EUR, and from EUR back to RIGS, will be the explicit and informed consent of the data subject (participant). The JCA model is hereby abandoned for this study.
- **Data Controller Roles:**
- **Participating Hospitals (including RIGS):** Act as autonomous Data Controllers for the initial collection of participants' email addresses and for obtaining the necessary consent to share them with EUR.
- **EUR:** Acts as the sole Data Controller for all personal data collected, processed, and stored via the Qualtrics platform.
- **RIGS (and other participating hospitals that wish to analyze answers given by their employees):** Acts as a Data Controller for the pseudonymized dataset it receives from EUR containing responses from its own employees.

- **Data Minimisation:** Only personal data strictly necessary for the research objectives will be collected. The pseudonymization technique will not use superfluous personal details (e.g., name, age, street number) and will instead rely on a randomized ID.

3. Data Processing Workflow

Step 1: Participant Recruitment at Participating Hospitals

- Each participating hospital is responsible for collecting the email addresses of interested participants.
- Before sharing, the hospital must provide participants with a dedicated privacy notice and obtain their consent to share their email addresses with EUR for the purpose of receiving an invitation to the study.

Step 2: Specific Procedure for RIGS (and other participating hospitals that wish to analyze answers given by their employees)

- In addition to the consent in Step 1, RIGS must obtain a second, specific consent from its participants (employees).
- This consent is required to authorise EUR to share their stronlgy pseudonymized (but potentially re-identifiable) individual responses back to RIGS for analysis.
- RIGS is solely responsible for ensuring it has the legal grounds to receive and process this special category of personal data belonging to its own employees.

Step 3: Data Collection and Pseudonymization by EUR

- EUR will use the provided email addresses to send a unique registration link for the Qualtrics platform to each participant.
- On Qualtrics, EUR will provide the full study privacy notice and obtain informed consent for both study participation and the processing of personal data.

- Each participant will be assigned a randomized, non-identifiable ID to ensure pseudonymization. This method replaces the previously outlined pattern to enhance participant privacy.

Step 4: Data Analysis and Sharing

- **Sharing with RIGS:** Upon receiving specific consent (as per Step 2), EUR will share the pseudonymized, individual-level dataset of RIGS's participants back to RIGS. This dataset must be treated as personal data due to the potential for re-identification through demographic and professional details.
- **Sharing with Consortium and Other Hospitals:** For all other participating hospitals and the wider consortium, EUR will only share fully anonymized and aggregated results. No individual-level or pseudonymized data will be shared with these parties, in line with the confidentiality commitment stated in the research protocol.

4. Implementation of Privacy Notices and Consent Collection

To operationalize the principles outlined above, the following privacy notices and corresponding consent collection mechanisms will be implemented by the relevant parties:

- **Study E_Privacy_Notice_EUR_study_administration**
- **Responsibility:** EUR.
- **Implementation:** This notice must be uploaded to the study platform (Qualtrics) and presented to each participant after they first log in but **before** they can access the questionnaire.
- **Consent Mechanism:** Access to the questionnaire will be conditional upon acknowledgement of the notice. This will be achieved with a gateway statement, such as: *"By clicking 'Continue' to proceed, you confirm that you have read and understood this privacy notice."*

- **Study E_Privacy_Notice_participating_hospitals_no_data_analysis**
- **Responsibility:** Participating hospitals that **will not** receive individual-level data for analysis.
- **Implementation:** This notice must be provided to participants at the point of recruitment, when their email address is collected.
- **Consent Mechanism:** The notice must be presented contextually with the request to obtain the participant's explicit consent to share their email address with EUR.
- **Study E_Privacy_Notice_participating_hospitals_with_data_analysis**
- **Responsibility:** RIGS and any other participating hospital that **will** receive its own pseudonymized, individual-level data for analysis.
- **Implementation:** This notice must be provided to participants at the point of recruitment.
- **Consent Mechanism:** The notice must be presented contextually with the request to obtain **two distinct consents** from the participant:
- Consent to share their email address with EUR.
- Consent to allow EUR to share their pseudonymized response data back to their employer hospital (e.g., RIGS) for analysis purposes.

5. Consent Collection Templates and Wording

This section provides the specific wording for the consent forms to be implemented at each stage of participant interaction, balanced for clarity and legal precision.

5.1 Consent Form for Participating Hospitals (Standard Model)

*To be used by hospitals that will **not** analyze their own data. This is presented after the participant has read the Study E_Privacy_Notice_participating_hospitals_no_data_analysis.*

[ ] I confirm I have read the provided privacy notice and give my consent for **[Name of Participating Hospital]** to process my **email address**. This will be done for the sole purpose of sharing it with EUR, who will then invite me to participate in Study E.

I understand that I have the right to withdraw this consent at any time by contacting [Contact email/office of the hospital]. The withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal.

5.2 Consent Forms for RIGS (or similar hospitals performing data analysis)

*This requires collecting **two separate consents**. These are presented after the participant has read the Study E_Privacy_Notice_participating_hospitals_with_data_analysis.*

Consent 1: For sharing your email address with EUR

[ ] I confirm I have read the provided privacy notice and give my consent for **[Name of RIGS or other analysing hospital]** to process my **email address**. This will be done for the sole purpose of sharing it with EUR, who will then invite me to participate in Study E.

I understand that I have the right to withdraw this consent at any time by contacting [Contact email/office of the hospital]. The withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal.

Consent 2: For the return of pseudonymized data to your hospital

[ ] I also give my specific consent for EUR to share my **pseudonymized, individual-level survey responses** back with my employer, **[Name of RIGS or other analysing hospital]**. I understand my employer will process this data for internal research and analysis.

I understand that I have the right to withdraw this consent at any time by contacting [Contact email/office of the hospital]. Withdrawal will prevent future data sharing but will not affect the lawfulness of analysis already completed.

5.3 Consent Form for EUR (on the Study Platform)

To be presented on the survey platform after the participant reads the Study E_Privacy_Notice_EUR_study_administration and immediately before the questionnaire.

Important Note: It is crucial to distinguish between the **Informed Consent for participation in the study** (an ethical research requirement) and the **consent for the processing of personal data** (a legal requirement under GDPR). The GDPR-specific consent text provided below is designed to supplement and be integrated with the broader Informed Consent form, which is already detailed in the approved research protocol. This ensures compliance with both regulatory frameworks.

[ ] By ticking this box and proceeding, I declare the following:

- I have read and understood the privacy notice provided by EUR for this study.
- I consent to **EUR** processing the personal data I provide in my survey responses for the research purposes of Study E.
- I give my explicit consent to the processing of **special categories of data, including information about my health**, which are collected in the questionnaire.
- I understand my right to withdraw this consent at any time by contacting [Contact email/DPO of EUR]. The withdrawal of consent will not affect the lawfulness of processing that occurred prior to the withdrawal.

Annex 2.5

Status: Planned. This annex will be added once produced.

Annex 2.6

JOINT CONTROLLERSHIP AGREEMENT

The Parties:
NUROMEDIA GMBH, PIC 968574392, established in Schaafenstrasse 25, KOLN 50676, Germany, hereinafter referred to as ["**NURO**"],
and
ECHALLIANCE COMPANY LIMITED BY GUARANTEE, PIC 907578852, established in 20 Harcourt Street Raheny, DUBLIN D02H364, Ireland, hereinafter referred to as ["**ECHA**"],

hereinafter collectively referred to as the "Parties" and individually referred to as a "Party",

Whereas:

- The Parties collaborate on the Europe-funded Project entitled KEEPCARING (the "Project") together with other partners;
- The Project is regulated by the Grant Agreement n.101137244;
- The aim of the Project is to (re-)build wellbeing and resilience of healthcare workforce in EU hospitals by co-creating a multi-faceted non-digital, digital and AI-supported solution package to prevent burnout among (aspirant) healthcare professionals on the individual;
- The Project's ambition is to safeguard and enhance the wellbeing and resilience of healthcare professionals in EU hospitals in surgical pathways by researching factors of influence on stress and resilience in order to help promote job engagement and retention;
- In order to achieve this purpose the Project will involve the collection, processing, and storage of various data sets;
- Under the Work Package ("WP") 6: "Dissemination, communication and maximising impacts" described in the Grant Agreement, in order to raise awareness of the (mental) wellbeing burden of health and care professionals and to improve visibility of the Project and findings to a wide range of stakeholders, a public website dedicated to the Project has been created;
- The Project website will provide (i) up-to-date information on Project aim, partners, approach, and results, regular news items and blog posts, (ii) interactive discussion and internal section where partners can share progress, (iii) the possibility to subscribe to the newsletter to receive updates, results, and upcoming events concerning the Project;
- In this context, the Parties are involved in the management of the website and collect, store, and share some personal data as defined by art. 4 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, ("General Data Protection Regulation' or "GDPR");
- Since the Parties jointly determine the purposes of the Data Processing Operations and the means used therein, they are joint controllers within the meaning of Article 26 of the GDPR and they must transparently determine, through an internal agreement, their respective responsibilities regarding the obligations stemming from the personal data processing legislation,

Now, therefore, the Parties have agreed as follows:

Art. 1. Definitions
The terms controller, joint controllers, data processor, processing, data subjects, data breach used in this agreement have the meaning indicated in the GDPR.

Art. 2 Scope of the agreement and personal data processing
2.1. This agreement is designed to enable the Parties to comply with the obligations of the GDPR related to the processing activities carried out for the purposes and with the means jointly determined as Joint controllers.
2.2. Joint controllership exists with respect to the data processed and used by the Parties within the scope of the Project for the purpose of achieving the goals of WP6, in particular of performing the dissemination and communication activities through the website https://keepcaring.eu/ and the newsletter.

Art. 3 Activities, legal bases and categories of data

3.1 In particular, for the purpose of managing the website, the interactions with the stakeholders through the website and the newsletters, the joint controllers will collect and use the following information:

Data categories	**Data subjects**
email address	Researchers, health and care professionals and students, hospital managers, policy makers, and funders, companies and general public
ip address	

3.2. Each of the Parties is responsible for the collection and the use of personal data. Each Party will handle the information received with the highest possible level of diligence and will share it only with the other Parties.
Only aggregated information about the subscribers and the interactions with the users' website will be shared with other KEEPCARING consortium partners for the purposes of the Project.

3.4. The legal bases for the processing of personal data are the following:

Purpose	Legal basis	Responsible Partner
sending the newsletter	data subjects' consent - Art. 6(1)(a) of the GDPR	ECHA
if necessary, to fulfil a legal obligation or an order from the Authority	fulfilment of legal obligations - Art. 6(1)(c) of the GDPR	NURO, ECHA
if necessary, to defend or establish the Parties' rights	legitimate interest in defending the Parties' rights (Art. 6(1)(a) GDPR)	NURO, ECHA
to provide the website services	legitimate interest to promote the Project and its activities - Art. 6(1)(f) of the GDPR	NURO

Art. 4 Lawfulness of processing and data subjects' rights

4.1. Each of the Parties undertakes to process the data in compliance with the GDPR and any other applicable national and supranational privacy and data protection laws. In particular, they must adopt all the necessary technical and organisational measures to ensure the exercise of data subjects' rights and that they answer to their requests in a timely manner.

4.2. When needed, the Parties are responsible for ensuring that there is a valid consent for processing the data and they must be able to demonstrate this.

4.3 The Parties will not collect more personal data than is strictly necessary for the purpose in question. The Parties will only process Personal Data for the purpose for which Personal Data was collected, unless the Parties agree, after consultation, that Personal Data may also be used for purposes that are sufficiently connected to the purpose for which it was collected

Art. 5 Data subjects' rights

5.1. Right to be informed. The Parties will make sure that data subjects receive the required information (as described in article 13 and 14 of the GDPR) when personal data is collected. They will make sure that data subjects know the name and the contact details of the joint controllers and of their data protection officers, the purposes of data processing, the legal basis for processing and be well informed about the data recipients and the retention period. All this information will be explained in a concise, transparent, intelligible and easily accessible form with clear and simple language. To this end, the Parties have agreed on the text of the privacy notice that will be provided to the website's users, which is attached here.

5.2. Right of access. The Parties undertake to respect and guarantee the right of access of the data subjects pursuant to Article 15 of the GDPR. The Parties acknowledge that the obligation to comply with a data subject's request lies with the Party to which the request was submitted, unless the data in question can be attributed to a specific controller. In such instances, that controller assumes this responsibility. Should it become necessary, the Parties will provide each other promptly with any reasonable assistance necessary (in any event within 5 working days of a request for assistance) to ensure requests are addressed and to respond to any other questions or complaints raised by Data Subjects.

5.3. Regardless of the internal arrangements, the Parties acknowledge that data subjects may exercise their rights under Articles 15 to 22 of the GDPR with regard to and against any of the Parties (Art. 26 (3) GDPR).

5.4. Right to erasure of data. If personal data must be deleted, the Parties shall inform each other in advance. A Party may object to the deletion for justified reasons, for example if it is subject to a legal obligation to retain the data.

5.5. Rectification of information. Each party is required to inform the others, within 5 days and completely, of any errors or irregularities in personal data protection provisions of which it has become aware during the examination of the processing activities and shall rectify them promptly.

5.6. The contact point to be contacted for the exercise of rights are:

NURO: Boris Uszko, Project Manager, Nuromedia GmbH, boris.uszko@nuromedia.com
ECHA: Dimitrios Georgoulis, Innovation Project Manager, ECHAlliance, dimitris@echalliance.com

5.7. Each party shall inform the others of any change regarding the indicated point of contact.

Art.8 Making the essential content of the agreement available to the data subjects

The Parties undertake to make available to the data subjects the essential content of this joint controllership agreement, at the data subjects' demand.

Art. 9 Security of processing and evidence of compliance with the GDPR

9.1 Parties will be responsible to implement appropriate technical and organisational measures to ensure and demonstrate that the processing is in compliance with the GDPR, taking into account the nature, scope, context and purposes of the processing involved, as well as the risks of varying degrees of likelihood and severity for the rights and freedoms of natural persons. The measures shall be reviewed and updated as necessary.

9.2 The Parties' measures shall include, where proportionate to the processing activities, the implementation of appropriate data protection policies.

9.3 The Parties shall be responsible for compliance with the data protection by design and data protection by default rule of Article 25 of the GDPR.

10. Use of data processors and sub-processors

10.1 The Parties are entitled to use processors and/or any sub-processors in connection with the joint processing operation.

10.2 In the event of use of processors and/or sub-processors, the Parties shall be responsible for complying with the requirements of Article 28 of the GDPR. Accordingly, inter alia:

1. use only processors that can provide the necessary guarantees that they implement appropriate technical and organisational measures in such a way as to ensure that processing complies with the requirements of the GDPR and safeguards the rights of the data subject,
2. ensure that a valid data processing arrangement is in place between the Party and the processor; and
3. ensure that there is a valid sub-processor arrangement between the processor and any sub processor.

10.3. The Parties may have Personal Data processed by other persons or organisations outside the European Economic Area, provided that the applicable laws and regulations regarding the Processing of Personal Data are observed.

10.4. The Parties have agreed to rely on Mailchimp as a data processor for the newsletter service.

11. Records of processing activities

11.1 Each Party is independently responsible for complying with the requirements of Article 30 of the GDPR on records of processing activities. Each Party shall report the processing activities carried out jointly and covered by this agreement in their own record of the processing activities.

12. Notification of personal data breaches to the supervisory authority

12.1 Each Party is and remains independently responsible for reporting any data breaches that take place under its responsibility to the Supervisory Authority and/or the data subjects, in accordance with Articles 33 and 34 of the GDPR.

12.2 Upon becoming aware of such a breach, a party must immediately inform all other parties within 24 hours, providing all relevant information about the breach necessary to make the notification. The notification must contain at least the following information:

- the nature of the personal data breach
- the categories and approximate number of the data subjects concerned
- the categories and approximate number of personal data records concerned
- the contact from which to obtain more information
- the description of the likely consequences of the breach
- the actions implemented or planned to be implemented to remedy the breach, and if applicable, a description of measures taken to mitigate any possible adverse effects.

12.3 The Parties will keep each other informed about the developments concerning the breach.
12.4 The Party where the breach occurred will bear any costs incurred for resolving the Breach, and for preventing any breaches in the future. The Parties may confer about a possible division of these costs if it concerns a solution that is in the interest of all the Parties.
12.5 The Parties are each responsible for keeping a data breach register.

13 Data protection impact assessment
13.1 The Parties shall be responsible for compliance with the requirement of Article 35 of the GDPR on data protection impact assessments ("DPIA").
13.2 The Parties acknowledge that the type of processing required by this phase of the Project is not likely to result in a high risk to the rights and freedoms of natural persons. For such reasons, the Parties will not carry out a DPIA for this phase.

14 Complaints
14.1 The Parties shall each be responsible for handling any complaints from data subjects, if the complaints relate to a breach of the provisions of the GDPR, for which the Party is responsible under this arrangement.
14.2 If one of the Parties receives a complaint, which should rightly be dealt with by the other Party, the complaint shall be forwarded to that Party as soon as possible.
14.3 If one of the Parties receives a complaint, part of which should rightly be dealt with by the other Party, that part shall be forwarded to the Party for reply as soon as possible.
14.4 The data subject shall be informed of the essential content of this arrangement when one Party forwards a complaint or part thereof to the other Party.

Art.15 Data Retention
Name and contact details of the newsletter's subscribers will be held for the duration of the Project and deleted after 2 (two) years from the end of the Project unless the subscriber withdraws the consent before. All the other information collected and used for the Project will be held by the Joint Controllers for ten years after the end of the Project.

Art. 16 Secrecy and confidentiality
16.1 All Personal Data is classified as confidential information and will be treated as such. The Parties will also impose this duty of confidentiality on all persons or legal entities that they engage, including but not limited to Employees, Processors, Third Parties and other Recipients of Personal Data.

16.2 The Parties will maintain the confidentiality of all Personal Data and will not disclose it in any way whatsoever either internally or externally, except insofar as:
(i) the disclosure and/or provision of the Personal Data is necessary in the context of implementing the Main Agreement or this Agreement;
(ii) a mandatory statutory provision or court order handed down by a competent court or order from any other governmental body having authority over the Parties obliges the Parties to disclose, provide and/or transfer this Personal Data. If this is the case, the Parties will first notify the other Parties in the process; or
(iii) disclosure and/or provision of this Personal Data is done with the prior Written permission of the other Parties.

Art.17 Final provisions
17.1 This arrangement shall enter into force upon signature by all Parties hereto.
17.2 The arrangement shall remain in force for as long as the data concerned are processed or until it is replaced by a new arrangement laying down the division of responsibilities in relation to the processing. Obligations ensuing from this Agreement that are, by their nature, intended to continue after termination of this Agreement will continue after this Agreement is terminated.
17.3 Any changes to this agreement must be made in writing and agreed between the Parties.
17.4 If one or more provisions of this Agreement should prove to be legally void, the rest of this Agreement will remain in force. The Parties will then confer on the provisions that are not legally valid, with a view to making an alternative arrangement that is legally valid and, as far as possible, corresponds to the purport of the provision being replaced.
17.5 A Party that imputably fails to comply with any of its obligations under the GDPR or this Agreement, and as a result of which the other Parties are held accountable for damages, costs or interest by a Third Party, will indemnify the other Parties in full against the claims of this Third Party, unless the Party proves that the incident was caused by intent or gross negligence on the part of the other Party or Parties.
17.6 The obligations arising from this Agreement will also apply to those who process personal data under the Parties' authority, such as its employees and processors engaged.

Place and date
09/04/2025

Dimitrios Georgoulis
Innovation Project Manager
ECHAlliance
dimitris@echalliance.com
[On behalf of ECHAlliance]

Cologne, 11.04.2025

Nuromedia GmbH
Schaafenstraße 25, 50676 Cologne, Germany
www.nuromedia.com, info@nuromedia.com
Phone: +49 221 398 80800, Fax: +49 221 398 8001
Trade Register: HRB 57289, Amtsgericht Köln
Tax ID: 214/5813/1355, VAT: DE814670158

Annex 1 Information on the processing of personal data for website's users

ANNEX 1

KEEPCARING WEBISITE PRIVACY NOTICE

WHO ARE WE?

This website is dedicated to the KEEPCARING PROJECT (the "Project").

The aim of the Project is to (re-)build wellbeing and resilience of healthcare workforce in EU hospitals by co-creating a multi-faceted non-digital, digital and AI-supported solution package to prevent burnout among (aspirant) healthcare professionals on the individual, team, and organisational level.

Among the dissemination and communication activities of this Project, this website has been created to raise awareness of the (mental) wellbeing burden of health and care professionals and to improve visibility of the Project and findings to a wide range of stakeholders

The Project's Partners which will process your personal data collected through the website are:

NUROMEDIA GMBH, established in Schaafenstrasse 25, KOLN 50676, Germany [**"NURO"**],
ECHALLIANCE COMPANY LIMITED BY GUARANTEE, established in 20 Harcourt Street Raheny, DUBLIN D02H364, Ireland [**"ECHA"**]

These organisations act as joint controllers of the data collected through the website and used for the dissemination and communications activities related to the Project and you can contact them for privacy related matters at contact@keepcaring.eu.

They have signed a joint controllership agreement and you can receive an abstract of this agreement by contacting them at the email addresses indicated above.

LINKS

This website may contain links to websites operated by third parties. We are not responsible and have no control over how they operate or how they process data. We encourage you to read their privacy notices before using those websites.

WHAT TYPES OF DATA DO WE PROCESS AND WHY?

1. Browsing data

The information systems and software procedures relied upon to operate this website acquire personal data as part of their standard functionalities; the transmission of such data is an inherent feature of Internet communication protocols.

This data category includes the IP addresses and/or the domain names of the computers and terminal equipment used by any user, the URI/URL (Uniform Resource Identifier/Locator) addresses of the requested resources, the time of such requests, the method used for submitting a given request to the

server, returned file size, a numerical code relating to server response status (successfully performed, error, etc.), and other parameters related to the user's operating system and computer environment.
This data is necessary to operate web-based services in a secure and stable manner. Data will be deleted immediately after the access or within ten days.
The legal basis of the processing (the legal requirement) to operate the website, is the legitimate interest of the KEEPCARING partners to promote the Project and its activities.

2. Data communicated by you
a) when you contact us: if you send an e-mail message to the email address indicated above we will process your data (name, e-mail address, content of the message) only to reply to your requests (the legal basis, i.e. the basis required by law for processing your data, is the necessity to perform the contract or to take steps at the request of the data subject prior to entering into a contract (Art. 6(1)(b) of the General Data Protection Regulation "GDPR").
b) when you subscribe to our newsletter: we will process your name, surname and e-mail address, to send you communications about our Project. The legal basis is your consent (Art. 6(1)(a) GDPR).

3. Data we use when we must comply with legal obligations or defend our right: if necessary, your data could be processed to fulfill a legal obligation. The legal basis of the processing is the necessity to comply with a legal obligation to which the controller is subject (Art. 6(1)(c) GDPR)
Sometimes we may also need to use your data to defend or establish our rights.
The legal basis of the processing is our legitimate interest in defending our rights (Art. 6(1)(a) GDPR).
In these cases, the data will be held for the time required by law or authority or for the time necessary to enforce or defend our right.

Cookies
Cookies are small text files stored on users' devices by the server of the website they are visiting and contain information about the user's navigation that can be read by the same server in subsequent browsing sessions. Cookies do not harm the device and enable a better browsing experience.
Our Website uses cookies. To know more about the cookies we use on our website, please refer to our Cookie Policy.

ARE YOU REQUIRED TO PROVIDE US WITH YOUR DATA?
As mentioned, browsing data is automatically acquired upon access.
On the other hand, you are not obliged to communicate with us. It's all optional. However, if you would like to receive an answer to your questions, you will need to provide us with the data indicated above.
Consent for the newsletter is always optional. If you refuse, you will not be updated on our updates, news and events concerning the Project.

WHO DO WE COMMUNICATE YOUR DATA TO?
We can communicate the data to our service providers which carry out some services on our behalf (such as hosting providers, email services providers and other IT services providers) as data processors in accordance with a data processing agreement.

We can communicate the data to other public or private bodies whenever we are obliged to do so to comply with law or regulatory requirements.

DO WE TRANSFER YOUR DATA?

We store your data in Europe. However, some of our suppliers when providing their services can access data from countries outside of the EU/EEA, such as Mailchimp (from US).

In these cases, data is transferred only in the presence of the safeguards indicated in the applicable data protection legislation. In particular, the transfer will take place:

-to destination countries for which the European Commission has issued an adequacy decision (art. 45 GDPR) or

- on the basis of the Standard contractual clauses ("SCCs") adopted by the EU Commission (art. 46 GDPR) provided that supplementary security measures are also in place.

For further information about the data transfers, you can contact the joint controllers at contact@keepcaring.eu.

HOW LONG DO WE KEEP YOUR DATA?

The data you provide us through spontaneous emails will be retained for the time needed to reply to you and, in any case, for a maximum of six months.

Your email address collected to send you the newsletter will be held for the duration of the Project and for further 2 years. However, you can withdraw your consent at any time and the joint controllers will stop the processing.

YOUR RIGHTS

You have certain rights in connection with the data processing.

You have the right to access your data and to modify or correct your data.

You can obtain the erasure of personal data and the restriction of the processing when certain conditions are met.

You have the right to receive a copy of your personal data in a structured, commonly used and machine-readable format or ask Us to transmit that data to another controller, where technically feasible, if the processing is based on consent or on a contract and is carried out by automated means.

You have the **right to withdraw the consent** you have given at any time, without affecting the lawfulness of the processing carried out before the withdrawal.

You can always **object to the processing** of your personal data for direct marketing purposes and, on grounds relating to your particular situation, you can also object to the processing of your personal data based on the legitimate interest of the controller.

You can lodge a complaint with the data protection authority of your country if you believe that your rights have been breached.

If you wish to exercise one of these rights, you can contact the joint controllers at contact@keepicaring.eu.

CHANGES TO THE PRIVACY POLICY AND OUR DUTY TO INFORM YOU OF CHANGES

We keep our privacy policy under regular review and may modify and revise it occasionally. Any information we collect is subject to the privacy policy in effect at the time such information is collected.

Any changes we make to our privacy policy in the future will be posted on this page and, where appropriate, notified to you by email. Therefore, we encourage you to review it from time to time to stay informed of how we process your data.

This policy was last updated on February 2025

CONSENT COLLECTION FOR NEWSLETTER

"I have read the privacy notice and by clicking subscribe I consent to receive the newsletter".

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.