REal-time data monitoring for **S**hared, **A**daptive, **M**ulti-domain and **P**ersonalised prediction and decision making for **L**ong-term Pulmonary care **E**cosystems

D4.8: Security and Data Protection Policies

Dissemination level:	Public
Document type:	Report
Version:	1.0
Date:	31.10.2023

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 965315. This result reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains.

Document Details

Reference No.	965315
Project title	**RE-SAMPLE** - **RE**al-time data monitoring for **S**hared, **A**daptive, **M**ulti-domain and **P**ersonalised prediction and decision making for **L**ong-term Pulmonary care **E**cosystems
Title of deliverable	Security and Data Protection Policies
Due date deliverable	31/10/2023
Work Package	WP4
Document type	Report
Dissemination Level	PU: Public
Approved by	Coordinator
Author(s)	Lambrinoudakis C. (UPRC), Kalloniatis C. (UPRC), Lyvas C. (UPRC), Kanatas A. (UPRC), Gritzalis S. (UPRC), Menegatos A. (UPRC), Giannakopoulos T. (UPRC)
Reviewer(s)	Florian Hahn (UT) and Danae Lekka (iSPRINT)
Total No. of pages	56

Partners

Participant No	Participant organisation name (country)	Participant abbreviation
1 (Coordinator)	University of Twente (NL)	UT
2	Foundation Medisch Spectrum Twente (NL)	MST
3	University of Piraeus Research Center (GR)	UPRC
4	Foundation Tartu University Hospital (EE)	TUK
5	Foundation University Polyclinic Agostino Gemelli IRCCS (IT)	GEM
6	European Hospital and Healthcare Federation (BE)	HOPE
7	German Research Center for Artificial Intelligence GMBH (DE)	DFKI
8	ATOS IT Solutions and Services Iberia SL (ES)	ATOS
9	Roessingh Research and Development BV (NL)	RRD
10	Innovation Sprint (BE)	iSPRINT

Abstract

The overarching goal of the RE-SAMPLE project is to leverage real-world data (RWD) to enhance the healthcare experience for patients dealing with Chronic Obstructive Pulmonary Disease (COPD) and coexisting chronic conditions. Additionally, it aims to establish a benchmark for caring for individuals with Complex Chronic Conditions (CCCs). The project utilizes this data to develop predictive models for identifying exacerbations and disease progression. These models empower both patients and healthcare professionals to make informed or shared decisions regarding proactive disease management, treatment, and lifestyle adjustments. Moreover, the project seeks to gain valuable insights into everyday factors that can trigger health issues, allowing for their mitigation and decreased occurrence. Machine learning (ML) is employed to explore the relationships between patients' clinical and non-clinical characteristics and their impact on disease progression.

The RE-SAMPLE platform takes a security and privacy-centric approach, ensuring the secure and privacy-preserving processing of clinical and non-clinical data in compliance with the General Data Protection Regulation (GDPR). In this context, it is imperative to present the policies that RE-SAMPLE's clinical partners must adhere to. These policies encompass the necessary organisational procedures, complementing the proposed technical security and privacy safeguards, to ensure GDPR compliance and substantial protection of patients against both intentional and accidental threats.

The main objective of this deliverable (including one more iteration that will follow) is to describe the data protection policy for the RE-SAMPLE platform. More specifically all the procedural and organisational measures for enforcing GDPR compliance are described based on the articles and principles that GDPR itself discusses. Finally, a set of template forms are provided in the appendix of the deliverable that aim to assist clinical partners in applying the proposed processes in the cases where input from patients is required.

Contents

List of Tables

List of Figures

Symbols, definitions, abbreviations, and acronyms

CCC	Complex Chronic Conditions
COPD	Chronic Obstructive Pulmonary Disease
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DPP	Data Protection Policy
GDPR	General Data Protection Regulation
IS	Information System
IT	Information Technology
ML	Machine Learning
PDBMT	Personal Data Breach Management Team
RWD	Real-World Data
VCP	Virtual Companionship Product
WP	Work Package

1. Introduction

The deliverable presents the data protection policy of the RE-SAMPLE platform. It is the result of the work performed in *Task 4.5 "Security & privacy measures, security & data protection policies"* and is linked with deliverable D4.7 *Measures for Organisational, Legal and Technical Security and Privacy Requirements* (and its updates D4.13 and D4.14) which presents the appropriate organisational, legal and technical measures for satisfying the respective legal, security and privacy requirements reported in D4.3 *GDPR related and Security/Privacy Requirements* (and its updates D4.10 and D4.11). More specifically the scope of the security and data protection policy for the RE-SAMPLE platform is to present in a clear and robust way the required organisational changes for the protection of personal data, procedures for acquiring user consent, withdrawal of consent, access control, managing security and privacy incidents, informing authorities, managing log files, privacy conditions for contracts entered into with staff, customers, suppliers and other GDPR related processes that ensure the effective enforcement of the regulation and the substantial protection of patient's data in RE-SAMPLE.

This deliverable includes all relevant information, in the form of processes/guidelines and templates, for designed to support RE-SAMPLE clinical partners in integrating them into their own policy framework. It is clear that all three clinical partners don't have to alter their existing Data Protection Policy, nor to adopt the RE-SAMPLE Data Protection Policy in parallel with their own, **provided that** their own Data Protection Policy fully satisfies all the requirements (in terms of obligations, procedures, templates, archives etc.) set by the RE-SAMPLE Data Protection Policy.

2. Objective

As D4.8 *Security and Data Protection Policies* is the first out of the two iterations of this deliverable the goal of this first iteration is to present what a data protection policy is and what it should contain in terms of the General Data Protection Regulation (GDPR). Subsequently, these principles will be applied on the RE-SAMPLE platform thus forming the official policy for all clinical partners of the project. Thus, **Section 3** presents a high-level description of the requirements that should be satisfied from an organisational and procedural point of view, in order to comply with GDPR but also safeguard patient's privacy. **Section 4** presents specific procedures that should be adopted by RE-SAMPLE's clinical partners (Data Controllers) following the data protection policy presented in Section 3. RE-SAMPLE clinical partners need to adopt the procedures missing from their existing data protection policy while it is not mandatory to strictly follow the policy presented in this deliverable. They may choose to follow alternative, equivalent processes. However, in this case, they should be able to present proof of applicability for every organisational/procedural measure presented in this deliverable. **Section 5** concludes this deliverable by summarizing the contribution to RE-SAMPLE project. Finally, **Section 6 (Appendices)** presents template forms for assisting the application of the proposed organisational/procedural measures. These forms can be adopted by clinical partners or they can apply their own equivalent forms (if they exist).

3. Data Protection Policy

3.1 The Data Protection Policy

3.1.1 Introduction

The Data Protection Policy (DPP) typically encompasses the data controller's defined purpose and objectives concerning the safeguarding of personal data. It also outlines the directives, processes, regulations, roles, and responsibilities associated with its protection. Within the RE-SAMPLE project, the directives, regulations, and procedures outlined in the DPP will be put into action through suitable protective measures. The enforcement of the DPP is obligatory for all stakeholders within the RE-SAMPLE project, whether they are directly or indirectly engaged in operational processes that involve the handling of personal data.

3.1.2 Purpose and Objectives of the Data Protection Policy

The DPP describes the set of rules that define how the data controller protects personal data, thus complying with the GDPR and protecting the privacy of the data subjects (in RE-SAMPLE case the patients). The purpose of the DPP is to provide strategic guidance to the data controller's management and staff for the protection of personal data when processing them.

With the help of the DPP, the data controller seeks to achieve the following goals:

- The protection of individuals whose personal data is processed by the organisation.
- The identification of the risks involved in the processing of personal data by the organisation.
- The implementation of rules and techniques in order to satisfy the fundamental rights of the individuals whose personal data is processed by the organisation.
- The compliance with the requirements set by the European and National legal framework.

The DPP attempts to define commonly accepted principles, ways and responsibilities governing the processing of personal data. The DPP is not only about technical or organisational issues, but it treats both categories with the same attention.

3.1.3 Policy Applicability

The DPP applies to all personal data processed by the data controller, using automated or non-automated means, as defined in Article 4 of the GDPR, as well as to all operational processes that involve processing of personal data.

The DPP applies to all stakeholders of the RE-SAMPLE project and the services provided by the data controllers (GEM, TUK, MST).

3.2 Data Protection Policy Management Procedures

3.2.1 Policy Communication

The DPP is approved by the senior management of the data controller and communicated to all employees and relevant associates / partners.

3.2.2 Roles and Responsibilities for the Policy Management

The data controller implements an organisational structure, according to which specific roles carry responsibilities for the protection of personal data. The framework includes at least the following roles:

- Data Protection Officer (DPO) (see Section 3.4)
- Information Systems' (IS) Lead Developer
- Information Technology (IT) Officer
- Information Systems Manager
- Information Systems Auditor

The aforementioned roles, with the exception of the Information Systems Auditor, may be assigned to the same person.

The specific competences, assumed by each role, in the protection of personal data and the implementation of this policy are conferred by the management and recorded.

3.2.3 Policy Review

The DPP is a dynamic document that requires continuous maintenance to remain aligned with any modifications in information systems and the evolving technical and social landscape. It is ensured that the DPP undergoes updates at least on an annual basis, and these revisions are duly documented. Additionally, whenever significant changes occur within the organisation or its IT systems, the DPP is promptly reviewed and updated. The senior management of the data controller delegates the responsibility for overseeing these policy reviews to the Data Protection Officer (DPO).

3.2.4 Policy Implementation Supervision

The execution of the DPP and the regulations stemming from it are evaluated through suitable control procedures established by the DPO.

3.2.5 Internal Audit

The data controller conducts an annual internal audit of the information systems, as well as the organisational, procedural, and technical safeguards outlined in the DPP. This audit process is documented. The primary objective of this internal audit is to assess adherence to the policy and its effectiveness in safeguarding personal data. The Information Systems Auditor is responsible for orchestrating the internal audit by creating an audit plan that encompasses all processes involving the processing of personal data, define the audit criteria, and ensure that the audit findings are accessible for the forthcoming policy review. The organisation's management selects the team of auditors and assigns their respective responsibilities in this process.

3.3 Data Protection Impact Assessment

3.3.1 Introduction

The data controller protects the personal data, taking into account the risk of processing for the rights and freedoms of natural persons, and the nature, scope, context and purposes of the processing. The DPO defines a Data Protection Impact Assessment (DPIA) method that meets the following specifications:

- Ensures that repeated impact assessments lead to consistent and comparable results.
- Identifies risks related to unauthorised access, modification, and deletion of personal data.
- Assesses risk levels, taking into account the threat’s likelihood of occurrence and the potential impact of the risk.

The organisation is required to document a comprehensive description of the method employed for conducting DPIA in an official record. The DPO is responsible for executing this method, and the organisation documents the outcomes of this implementation in a separate document.

3.3.2 Frequency and Implementation Triggers

The DPO defines both the criteria and the triggers for initiating a DPIA, ensuring it is conducted whenever there are substantial developments or modifications in the organisation's operations or the methods of processing personal data. Additionally, regular data protection impact assessments are conducted, with the frequency determined by the DPO. However, the assessment cannot be conducted at a frequency less than a year.

3.4 Data Protection Officer (DPO)

3.4.1 Data Protection Officer

The senior management appoints a DPO, a qualified individual who reports directly to senior management without receiving specific instructions on how to carry out their duties as a DPO. The senior management is responsible for ensuring that the DPO is not subjected to dismissal or penalties for performing their tasks.

The DPO should have direct access to senior management, and individuals whose personal data is processed should have clear avenues for reaching out to the DPO.

While the DPO may have other responsibilities, the organisation takes measures to prevent any conflicts of interest arising from these additional professional roles and obligations.

The DPO holds responsibility for all matters that pertaining to the safeguarding of personal data within the organisation. Therefore, he/she must have access to all databases and the organisation's systems, all while adhering to strict confidentiality agreements.

3.4.1.1 Knowledge and Skills of the Data Protection Officer

The DPO is required to possess a range of knowledge and skills, including:

- **Specialized Legal Knowledge:** He/She should have in-depth expertise in the legal framework governing personal data protection at both the national and European levels.
- **Information Systems and Security:** Basic knowledge of information systems and information systems security is necessary to comprehend, design, and oversee the implementation of a personal data protection plan.
- **Communication Skills:** Effective communication skills are essential for reporting directly to senior management and persuading them to support compliance and the personal data protection plan.
- **Team Coordination Experience:** Experience in coordinating an internal team responsible for the personal data protection plan is valuable. He/She may serve as the team leader in this regard.
- **Proof of Competence:** The DPO should be able to demonstrate the adequacy of his specialized knowledge and experience in the field of personal data protection.

These qualifications and competencies are crucial to ensure effective oversight and compliance with data protection regulations within the organisation.

3.4.1.2 Tasks of the Data Protection Officer

The organisation assigns to the DPO the following responsibilities:

- **Representation to Authorities:** Acting as the organisation's representative in interactions with both national and European authorities in matters related to data protection.
- **Advisor to Senior Management:** Providing guidance and advice to senior management on data protection issues.
- **Policy Recommendations:** Proposing appropriate data protection policies directly to senior management.
- **Project and Service Monitoring:** Overseeing and ensuring alignment of the RE-SAMPLE project and services provided by RE-SAMPLE data controllers with data protection policies, practices, and methodologies for processing, storing, and transferring personal data.
- **Risk Mitigation:** Protecting RE-SAMPLE data controllers from the potential risks of substantial administrative fines as stipulated by personal data protection regulation.
- **Budget Support:** Securing the necessary support from senior management and the required budget for the implementation of the data protection program.
- **Program Development and Supervision:** Developing the data protection program and policy and supervising their implementation. Evaluating participation and success levels and making any necessary corrections.
- **Personal Data Inventory:** Establishing an inventory of personal data categories, including the type of personal data, storage and processing methods, retention periods, and data deletion or destruction procedures.
- **Impact Assessment:** Assessing and providing guidance on the creation of a DPIA method and conducting the DPIA on a case-by-case basis.

- **Interdepartmental Collaboration:** Coordinating collaboration across various departments, including Human Resources, Information Security, Information Systems, Legal and Regulatory Compliance, Marketing, and Procurement, to foster a sustained corporate culture of data protection as a valuable asset.
- **Training Programs:** Designing and implementing internal training programs and maintaining records of completed training by department or employee groups.

3.5 Lawfulness of Processing

3.5.1 Review the Lawfulness of Processing

The data controller adheres to a distinct procedure for identifying the various types of data being processed, including personal data, special categories of data, and data related to convictions, among others. Simultaneously, they must be capable of demonstrating that the processing methods employed are in accordance with the relevant processing guidelines and instructions applicable to each specific data type.

3.5.2 Consent as a Legal Basis for the Processing of Personal Data

The organisation records the legal basis for the processing of personal data. When *consent* is the legal basis, it is provided by the data subject freely, it is specific and clear. A prerequisite is that the data subject has been already informed about the purposes of processing.

3.5.2.1 Consent Management

The consent procedure will be user-friendly in order to avoid ambiguities. The data subject must be offered the option to withdraw its consent at any time.

Furthermore, it will be ensured that, at any time, the data subjects have access to their current status of consent and that they can modify it.

3.5.2.2 Consents' Record

The data controller must be able to demonstrate that the data subjects' consents have been recorded, including the interaction among the data subject and the data controller. The minimum information that should be maintained is:

- The identity of the data subject
- The date and time that the consent was obtained
- The location and the content of the consent

The consents' repository should be protected against malicious acts and should be available in case of audits.

3.5.3 Providing Information to Data Subjects

Prior to obtaining the data subjects' consent, the data controller will inform them at least for all the essential elements of the processing:

- The identity and contact details of the data controller.
- The identity and contact details of the DPO.
- The purposes and legal basis of the processing.
- Third parties and recipients potentially involved in data processing.
- The data retention period.
- Potential cross-border transfers.
- The data subjects' rights.

Furthermore, the information will be visible, easily accessible and understandable.

In cases where the personal data has not been collected directly by the data subjects, the data controller should inform them about the origin of the data.

3.5.4 Secondary Data Usage

If the data controller plans to process the data for a purpose different from the one for which it was collected, he/she will inform the data subjects and will renew their consent.

3.5.5 Children Consent

The data controller will follow a special procedure for obtaining the consent when the data subject is a minor.

3.5.6 Maintaining Data Quality

The data controller maintains the quality of the data by fulfilling data subjects' right to data rectification.

3.5.7 Data Minimisation

The data controller ensures that the processed data is the absolute minimum required for the fulfilment of the processing purposes.

3.5.8 Data Retention

For each purpose of processing, the data controller checks / determines the retention period for the processed data.

3.5.9 Maintaining Records of Processing Activities

The data controller keeps a detailed record of all processing activities under its responsibility. To achieve this, it is recommended to create a comprehensive inventory of enterprise information resources (referred to as a data inventory) and implement an appropriate data classification system. This record includes essential information such as the contact details of the data controller, the purposes of processing, a description of the categories of data subjects, a breakdown of the categories of personal data being processed, and a general overview of the technical and organisational security measures in place.

3.6 Data Subjects' Rights Fulfilment

3.6.1 Right to Information

Where personal data is collected directly from the data subjects, the data controller shall, at the moment when personal data is obtained, provide the data subjects with all of the following information:

- The identity and contact details of the data controller.
- The contact details of the DPO.
- The purposes of processing for which the personal data have been collected.
- The legal basis for the processing of personal data.
- The recipients or the categories of recipients of the data.
- (Where applicable) the intention of the data controller to forward the data to a third country or international organisation.
- The retention period of the data, or the criteria that determine the retention period.
- The right of users to submit a request to the data controller for exercising their rights (access, correction, deletion, limitation of processing, refusal of processing, data portability).
- The right to withdraw their consent.
- The right to submit a complaint to a supervisory authority.
- (Where applicable) The legal or contractual obligation or requirement, to sign a contract that (potentially) obliges the data subject to provide its data and the possible consequences of non-provision.
- (Where applicable) The existence of automated decision-making mechanism(s) (including profiling).

Furthermore, if the data controller intends to use the data collected for purposes other than those for which the data was collected, he/she must provide to the data subject information for that purpose.

If the data of the data subjects has not been collected by the data subjects themselves, the data controller, in addition to the above points, is obliged, within a reasonable time from the collection, but not later than one month, to include in the above procedure information on:

- The source from which the data is originating (if applicable, a reference to the source, if it is accessible by the public).

3.6.2 Right of Access

Data subjects have the right to request confirmation from the data controller regarding the processing of their personal data. If personal data is being processed, the data subjects have the right to access this information through a procedure facilitated by the data controller. This access includes the following details:

- **Purposes of Processing:** The reasons for which the personal data was collected and is being processed.
- **Data Categories:** The specific categories or types of personal data being processed.
- **Recipients of Data:** Information about who the personal data may be shared with.
- **Data Retention Period:** The duration for which personal data will be stored.
- **Rights to Correct, Delete, or Limit Processing:** Awareness of the data subject's right to request corrections or deletions of their data, or to limit its processing, as well as how to exercise these rights.
- **Right to Lodge a Complaint:** The right to file a complaint with the relevant supervisory authority.
- **Data Origin:** Clarification regarding the origin of the data, particularly when it was not directly collected from the data subject.
- **Automated Decision Making:** Information about the existence of automated decision-making processes, including profiling, if applicable.

3.6.3 Right to Rectification

The data controller follows a procedure through which the data subjects are able to correct or request correction of, at no cost, the personal data that the organisation maintains for them.

3.6.4 Right to Erasure

The data controller follows a procedure through which the data subjects can erase, or request the erasure, at no cost, of the personal data the data controller holds for them.

3.6.5 Right to Restriction of Processing

The data controller has established a procedure that allows data subjects to request the restriction of processing for their personal data. Once processing has been restricted, the data controller will require the consent of the data subjects to resume processing their data. In the event that the restriction of processing is lifted, the organisation is obligated to inform the data subjects accordingly.

3.6.6 Right to Data Portability

The data controller follows a procedure through which the data subjects can transfer or request the transfer of their personal data, at no cost, to another organisation.

3.6.7 Right to Object

The data controller follows a procedure through which the data subjects can declare their objection to the processing of their data, including user profiling.

3.6.8 Procedure for Managing Requests of Natural Persons

The data controller has prepared appropriate forms that can be used by the data subjects to submit a claim that falls under their rights (sections 3.6.1 - 3.6.7). These forms are available at a public point, either physically on the organisation’s premises or on its website.

3.6.9 Roles and responsibilities for the Rights of Data Subjects

The DPO is responsible for handling requests from data subjects. The data controller is required to promptly respond to data subject requests, providing all relevant information within one month from the date of

receiving the request. In exceptional cases where the request is complex or involves a large number of requests, an extension of up to two months may be necessary to fulfil the request.

3.7 Transfer of Personal Data to Third Countries

The data controller is permitted to transfer personal data to other organisations located in third countries or international organisations that adhere to GDPR compliance standards. Additionally, data can be transferred to jurisdictions that have been recognized as "adequate" for data protection or to organisations that demonstrate sufficiency through approved company rules.

In cases where the data controller intends to transfer personal data to third countries, they must store the data in a database in a format that can be easily exported to common standards, such as XML, JSON, Excel tables, etc. This facilitates data transfer while ensuring data protection and compliance with GDPR requirements.

3.8 Management of Third Parties – Data Processors

If the data controller intends to use data processors (third parties that will conduct personal data processing in their behalf), it shall select those who provide sufficient assurance that appropriate technical and organisational measures are applied to enable the processing to comply with the requirements of the GDPR. The collaboration contract/agreement between them regulates the obligations of each party.

3.9 Implementation of Data Protection by Design and by Default

3.9.1 Specifications for Data Protection by Design and by Default

During the development of new IT systems, the data controller has the responsibility to identify technical measures for safeguarding personal data. To achieve this, the Information Systems Development Officer collaborates with the DPO and selects a development approach that facilitates the identification and modelling of data protection mechanisms during the analysis phase of the overall system's specifications before implementation begins.

Additionally, the Information Systems' Lead Developer is tasked with ensuring that, from the outset, only the personal data required for the specific purpose is processed. Simultaneously, it is essential that the "default" settings of the applications are designed to be as privacy-friendly as possible. This approach promotes data protection and privacy at the core of the system's design and operation.

3.9.2 Procedures for Systems Procurement

The data controller is responsible for ensuring that, when acquiring new systems, appropriate technical measures for the protection of personal data are adhered to. In this process, the Information Systems' Lead Developer seeks guidance from the DPO and ensures that each procurement notice for a new IT system includes obligations for the contractor to identify and model personal data protection standards. Furthermore, the contractor is required to integrate these specifications into the new system during its development.

In addition, the organisation's Information Systems vendors are expected to demonstrate their adherence to the legal principles required in the solutions they provide for the organisation. This aspect should receive special attention when recording specifications and establishing evaluation criteria for the procurement of a new Information System. It underscores the importance of selecting vendors who prioritize data protection and compliance with legal requirements in their solutions.

3.10 Personal Data Breach Response Plan

The data controller maintains:

- A personal data breach response plan
- A notification plan for the data subjects and the supervisory Data Protection Authority (DPA)

The data controller is considered to become aware of a data breach as soon as it is established that an event has occurred that has impacted personal data. During the initial stages of investigating an incident, that should commence promptly, the data controller is not considered to possess knowledge of the breach. Whether it becomes immediately evident that personal data is compromised or if it takes some time to ascertain this fact, the primary focus should be on initiating a thorough investigation of the incident to determine whether a breach of personal data has indeed occurred.

3.10.1 Notification to the Supervisory Authority

When a data breach occurs, and provided that there is a risk for natural persons, the data controller must inform the competent supervisory authority "without delay and, if possible, no later than 72 hours from the time it occurred".

3.10.2 Procedures for Timely Notification

The data controller has defined procedures that describe how the communication with the supervisory authority is achieved and what information will be communicated to the authority. The organisation must state:

- The nature of the violation, including, if possible, the categories and number of affected data subjects, and the categories of data.
- The name and contact details of the DPO.
- The possible impact of the violation.
- The controls taken or proposed to be taken to address the breach.

3.10.3 Informing the Data Subjects

The data controller is required to inform data subjects in the event of a data breach, specifically when the breach could potentially pose a high risk to their rights and freedoms. The data controller has established procedures outlining how it communicates with data subjects and the content of the information that will be conveyed to them. This information must meet specific criteria, including being concise, transparent, easily comprehensible, and readily accessible. These requirements ensure that data subjects receive clear and understandable notifications regarding data breaches, enabling them to take appropriate actions to protect their rights and privacy.

3.10.4 Procedure for Managing IS Failures

The data controller employs suitable technologies to monitor its critical information systems responsible for managing personal data. In cases where a data breach arises due to a failure of these Information Systems, the organisation follows a proper procedure to both substantiate and document the security mechanisms it has put in place. This procedure ensures that the organisation can assess the breach, understand the underlying causes, and provide evidence of the security measures taken to prevent such incidents. It is a crucial step in maintaining accountability and demonstrating compliance with data protection regulations.

3.10.5 Roles and Responsibilities for Handling Personal Data Breaches

The data controller has established an internal incident response team, which includes representatives from all departments within the organisation. This team is entrusted with the task of swiftly containing, addressing, and facilitating the recovery of the organisation's operations in the event of an incident.

To ensure effective functioning, the roles and responsibilities of each team member must be clearly defined. It is proposed that the DPO assumes the role of the team's chief operating officer, providing leadership and expertise in data protection matters.

One critical aspect of the team's responsibilities is to thoroughly document the evidence related to each incident. This documentation is essential for conducting investigations, assessing the impact, and implementing measures to prevent future incidents.

3.11 Processing Personal Data for Research Purposes

Research activities are granted a special status under the GDPR. Consequently, there are various deviations and exceptions regarding the processing of personal data for research purposes. It's important to note that these exceptions are not automatically applicable but are assessed on a case-by-case basis. Specifically, deviations and exceptions for the processing of personal data for research purposes are considered when the following is given:

- **Appropriate Safeguards:** The processing is conducted with appropriate technical, organisational, and data protection measures in place, including principles such as minimization, pseudonymization, and logical access control.
- **No Adverse Impact on Individuals:** The processing does not lead to measures or decisions that would adversely affect individuals.
- **No Significant Harm or Danger:** The processing does not pose significant harm or danger to the rights and freedoms of data subjects.
- **Protection of Research Objectives:** Implementing the GDPR requirements may substantially hinder or even render impossible the achievement of the research objectives.

Purpose limitation: In the context of scientific research, the further processing of personal data is generally not considered incompatible with the original purposes for which the data were collected. This means that personal data collected by the data controller can indeed be used for research purposes, as long as appropriate safeguards and guarantees for the rights and freedoms of the data subjects are put in place. This approach recognizes the importance of facilitating research activities while also upholding data subject rights and privacy protections.

Limitation of the storage period: Personal data utilized for research purposes are indeed exempted from the GDPR requirement regarding their retention only for the duration necessary to achieve the specific processing purpose or as mandated by law. This implies that this data can be retained for extended periods, provided that they continue to be processed for scientific research purposes, and the appropriate measures and safeguards are implemented to protect the rights and freedoms of the data subjects. This approach recognizes the unique nature of research activities and allows for the retention of data beyond typical time limits, as long as they are handled in a manner that respects privacy and data protection principles.

Processing special categories of personal data: Processing special categories of personal data, i.e. the data of Articles 9 and 10 of GDPR (as these are the articles describing the special categories of data), is exceptionally possible for research purposes, which are proportionate to the intended purpose and respect the constitution right to data protection.

Transparent information to the data subjects: There are two deviations regarding the transparent information to the data subjects.

1. **Flexible Consent for Data Collected Directly:** When data has been collected directly from data subjects and is intended for a purpose different from the original one, especially in the context of scientific research, there is flexibility in the information provided to data subjects. This is because it can be challenging to precisely determine the purpose of processing personal data in scientific research from the outset. Data subjects can consent either to the overall research purpose in a more general manner or to specific areas or stages of the research.
2. **Exemption for Data Collected Indirectly:** In cases where personal data has not been collected directly from data subjects but through third-party sources (e.g., public sources, other public authorities), the researcher is not obligated by the Regulation to inform data subjects when doing so is impossible or would require disproportionate efforts. This exception is also applicable when such information could substantially hinder or even prevent the achievement of the research objectives. However, the required information must be made available to the public, and the researcher must implement suitable measures to safeguard the data of the subjects.

Data subjects' rights: When the processing of personal data is carried out for research purposes, the GDPR provides the possibility to EU Member States to predict deviations from the rights that data subjects may exercise. In particular, these deviations may concern the right of access, the right of rectification, the right to restrict processing and the right to object. Deviations are only applicable if these rights may harm or turn impossible the scientific research objectives. In addition, GDPR explicitly states that in cases where data processing is necessary for scientific research purposes, the right of erasure is not applicable.

3.12 Personnel Awareness and Training

The data controller ensures the regular provision of suitable awareness initiatives to personnel who handle or manage personal data, tailoring these actions to the specific roles of each employee. Additionally, users of the relevant Information Systems are equipped with the requisite resources, including manuals and tools, to ensure the proper and secure utilization of Information Systems responsible for managing personal data.

Furthermore, the organisation conducts regular training for qualified personnel, such as IT staff, to enhance their proficiency in developing, utilizing, and maintaining software, applications, and hardware that align with data protection standards and compliance with the GDPR. This comprehensive approach underscores the organisation's commitment to data protection and ensures that its personnel are well-prepared to handle personal data securely and in accordance with regulations.

3.12.1 Personnel Awareness

The data controller takes measures to ensure that all personnel within the organisation are informed about the current version of the DPP. This includes raising awareness among employees about their individual responsibilities pertaining to the implementation of the policy. Additionally, employees are made aware of the penalties and consequences that may be imposed in the event of violating the policy. This approach emphasizes the importance of data protection awareness and accountability throughout the organisation.

3.12.2 Training of Specialised Personnel

The data controller takes steps to ensure that the organisation's personnel possess the necessary knowledge and skills to effectively implement the DPP. This includes conducting regular assessments of the relevant knowledge and skills, with evaluations occurring at least annually.

The organisation also ensures that appropriate training and education are provided as needed to enhance the capabilities of specialized personnel. Furthermore, the effectiveness of these training initiatives is assessed to ensure that personnel are adequately equipped to fulfil their data protection responsibilities. This approach underscores the commitment to ongoing learning and competence-building in data protection practices.

3.13 Monitoring and Performance Measurement

3.13.1 Procedures for Monitoring Compliance with the Legislative and Regulatory Framework

The data controller can provide evidence of implementing suitable mechanisms to continually monitor its compliance with legal requirements. This involves the active involvement of both the organisation's legal department (or its legal partners) and the Information Systems' Lead Developer. These stakeholders oversee the policies and processes that have been established, as well as the technologies in place for ongoing monitoring and evaluation of security vulnerabilities.

This approach ensures that the organisation remains vigilant in upholding data protection and security standards, allowing for timely identification and mitigation of potential risks and vulnerabilities as they evolve over time. It also demonstrates a proactive commitment to compliance with legal requirements.

More specifically, the data controller ensures compliance with the GDPR requirements as shown in Table 1 below:

Table 1: Data Controller Obligations

Obligations	Procedures
Apply all necessary technical and organisational measures for ensuring that data subjects can exercise their rights	Section 3.6
Notify about acts that are related to the correction or deletion of personal data, or to the restriction of processing	Section 3.6.1
Consider protection of personal data from the design stages of the processing (privacy by design): Employ appropriate privacy and personal data protection technologies during the design phase of the processing rather than ex post, considering the latest technological developments, the cost for implementing the measures, the nature, scope, context and purposes of processing, and the minimization of risks that may affect the rights and freedoms of individuals during the processing.	Section 3.9
The "default" settings should be privacy-friendly. The IT Officer should define the necessary controls to ensure that the products comply with the privacy by default principle.	Section 3.9
Keep records of the processing activities. This obligation does not apply to an organisation employing fewer than 250 employees unless: - The processing being performed may cause a risk to the Data Subject's rights and freedoms. - Processing is not occasional. - Processing includes special categories of data. - Processing includes personal data relating to criminal convictions and offenses.	Section 3.5.9
Cooperate with the supervisory authority regarding: - Guidelines, recommendations, best practices - Regulatory actions - Codes of ethics - Certifications - Activity logs - Impact assessment on data protection - Data Transfers - Data Breaches - Audits - Corrective actions	Section 3.4
Ensure the confidentiality and security of the processing: - Use appropriate technical and organisational measures such as: o Pseudonymisation and encryption. Ensuring secrecy, integrity, availability and reliability. o Restoring availability and access in the event of an incident. Testing, assessing and continuous evaluation of the effectiveness of the measures	Deliverable D4.14 "Measures for Organisational, Legal and Technical Security and Privacy Requirements 2nd Update"
Notify, within 72 hours of becoming aware, the Supervisory Authority about personal data breaches, unless if the breach is not likely to endanger the rights and freedoms of natural persons.	Section 3.10.1
Carry out a DPIA - With regard to the impact assessment on data protection, the Controller should: o Have systematically described the processing activities envisaged, the purposes of the processing and the legal basis for them	Section 3.3 D4.11: GDPR related and Security/Privacy Requirements – 2nd update

Obligations	Procedures
○ Assess the necessity and proportionality of processing activities ○ Evaluate the risks to the rights and freedoms of the data subjects ○ Plan appropriate risk management measures - If, after the impact assessment on data protection has been carried out, there is still a "high risk", the data controller should consult the supervisory authority	
Designate a DPO, since: - The data controller's main activities require regular and systematic monitoring of the data subjects on a large scale. - The data controller's main activities are large scale processing of special categories of personal data.	Section 3.4

3.13.2 Procedures for Evaluating the Effectiveness of the Data Protection Policy

The data controller has implemented a plan to monitor and assess the effectiveness of the DPP through regular management reviews. This plan incorporates the following key components:

- **Performance Metrics:** The plan includes performance metrics related to the fulfilment of data subjects' rights and overall compliance with the GDPR. These metrics serve as benchmarks for evaluating the effectiveness of the policy.
- **Monitoring Methods and Techniques:** It outlines the methods and techniques to be used for monitoring and gathering relevant information. This may encompass various data collection methods, audits, assessments, and feedback mechanisms.
- **Frequency of Measurements:** The plan specifies the frequency at which measurements, data analysis, and evaluations will be conducted. This could be on a regular schedule, such as quarterly or annually, to ensure ongoing monitoring and assessment.

By incorporating these elements into the plan, the data controller can systematically evaluate the performance of the DPP, make necessary adjustments, and ensure continued compliance with GDPR requirements while safeguarding the rights of data subjects.

4. RE-SAMPLE Data Protection Policy

4.1 Data Protection Policy

In this section the policy and the respective procedures that RE-SAMPLE data controllers (clinical partners) must follow in order to protect patients' personal data and comply with GDPR are presented. RE-SAMPLE data controllers process personal data and special categories of personal data to support the purpose of processing **" Design, implement and evaluate the VCP to support patients with COPD and CCC and the HCPs that treat them"**. The personal data collected are processed by:

- the three clinical partners (each partner processes each one data)
- DFKI, UT and iSPRINT as data processors based on data processing agreements signed among them and the data controllers.

The following sections describe dedicated procedures that should be applied in order to safeguard the correct application of the policy described in Section 3. Three of these processes, *Handling of personal data breaches, lawfulness of processing and fulfilment of data subjects' rights* were designed and initially presented in Deliverable D4.7 "*Measures for organisational, legal and technical security and privacy requirements*" and in their respective iterations (Deliverables D4.13, D4.14) since they have a high impact on the measures that will be selected during the implementation of the RE-SAMPLE platform.

4.2 Handle Personal Data Breaches Procedure

4.2.1 Personal Data Breach Management Team (PDBMT)

The responsibility for establishing the Personal Data Breach Management Team (PDBMT) falls upon the DPO and the individuals in charge of the RE-SAMPLE data controllers (top management). The DPO is an integral member of the PDBMT, and the team is further comprised of system administrators, system owners, and all other relevant categories of technical personnel who have received appropriate training to effectively address potential breaches. This collaborative team approach ensures that the organisation is well-prepared to respond to and manage personal data breaches when they occur.

4.2.2 Criticality of the Personal Data Breach

The PDBMT evaluates security incidents and considers them as personal data breaches when they are likely to result in the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Furthermore, the PDBMT classifies the data breach with respect to the criticality of its impact as shown in Table 2.

Table 2: Criticality of the Personal Data Breach

Breach Category	Possible Impacts
Top Priority	- Loss of supporting assets which are critical for the RE-SAMPLE functionality. - Incident that leads to interruption of RE-SAMPLE services. - Large-scale unauthorised disclosure or access to specific categories of personal data processed by the RE-SAMPLE platform.
Medium Priority	- Loss of supporting assets which are important for the RE-SAMPLE functionality. - Incident that leads to significant downgrading of RE-SAMPLE services (e.g., denial of service attacks, malware). - Unauthorised disclosure or large-scale access to personal data processed by the RE-SAMPLE platform (e.g. privileged accounts breach).
Low Priority	- Incidents that are likely to lead to data integrity or availability breach, without, however, resulting in personal data leakage. - Loss of individual supporting assets (e.g. individual user account breaches, inability to use individual workstations).

Breach Category	Possible Impacts
	- Indications for attacks against the RE-SAMPLE platform (e.g. small number of failed unauthorised access attempts).

4.2.3 Procedure to Handle Personal Data Breaches

In case of a personal data breach that endangers the rights and freedoms of the data subjects (patients), the data controller must inform the Data Protection Authority (DPA) without any delay.

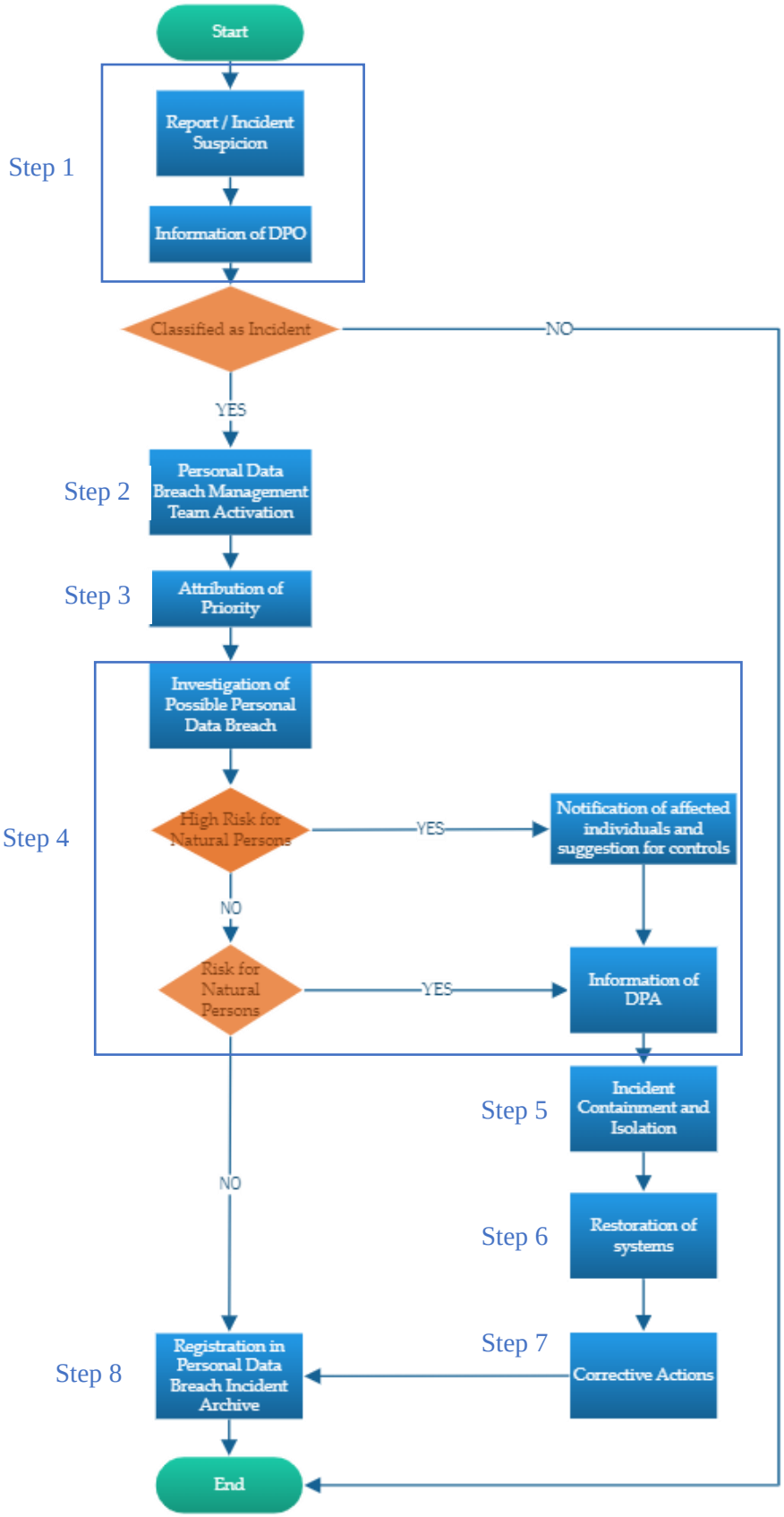

Figure 1: Procedure for handling personal data breaches

The steps that the RE-SAMPLE data controllers should follow for handling the data breaches are depicted in Figure 1 and listed next:

Step 1: Inform the DPO about a Suspected Incident
The DPO of the data controller serves as the central point of contact for receiving reports of suspected incidents, including personal data breaches. The contact details of the DPO, such as phone number and email address, should be communicated to all personnel and associates within the organisation. Suspected incidents can be reported in the following order of preference:

- Electronically, using the template form of Section 6.4.
- Electronically, by sending an email to the DPO.
- By phone, in exceptional cases where very serious incidents necessitate immediate attention.

After the DPO assesses the incident, he/she may activate the PDBMT and proceed to **Step 2**. Otherwise, the procedure is completed.

Step 2: Activate the PDBMT
The DPO informs the PDBMT.

Step 3: Priority assignment
The PDBMT assigns a priority to the incident, based on the potential impact and criteria listed in Table 2.

Step 4: Investigating personal data breaches and notifying the DPA and data subjects
The PDBMT promptly initiates an investigation into the breach to ascertain whether personal data is at risk or has been compromised. Given the potential threat to the rights and freedoms of data subjects, the data controller expeditiously notifies the DPA, ideally within 72 hours of becoming aware of the breach. The report to the DPA includes the following essential information:

- **Description of the Breach:** This description outlines the nature of the personal data breach, including details about the affected categories of personal data and an approximate number of data subjects impacted. Additionally, it should provide information about the categories and an approximate number of affected personal data files.
- **Contact Information:** The report includes the name and contact details of the DPO or another designated contact point from which more information can be obtained.
- **Expected Impact:** A description of the anticipated impact of the personal data breach, highlighting the potential consequences for data subjects.
- **Countermeasures:** Information about the countermeasures that have been implemented or are planned to address the personal data breach.

In addition, if there is evidence that the personal data breach may pose a high risk to the rights and freedoms of the data subjects, the data controller must immediately inform the data subjects about the incident by providing the following information:

- The name and contact details of the DPO, or other contact points from which more information can be obtained.
- The possible consequences of the personal data breach.
- The countermeasures taken or proposed / planned to be taken to address the personal data breach.

Step 5: Containment and isolation of the incident
To prevent any further propagation of the problem or potential destruction of evidence related to the incident, the PDBMT takes the following steps:

- **Isolation**: The PDBMT isolates the affected system, service, or supporting material that is under investigation. This isolation is crucial to contain the incident and prevent its spread to other parts of the organisation's infrastructure.
- **Immediate Actions**: The team swiftly undertakes immediate actions to isolate the source of the incident. This may involve tasks such as resetting network router settings or removing malware to stop the breach from continuing or worsening.
- **Evidence Collection**: Simultaneously, the PDBMT begins the collection of evidence related to the incident and its effects. This evidence-gathering process encompasses a thorough examination of systems, applications, hardware, and data to gather crucial information and artifacts.

These actions are vital in responding effectively to the incident, minimizing its impact, and preserving evidence for further investigation and reporting to relevant authorities.

Step 6: Applying system recovery and resetting the system
Once the investigation and evidence collection are completed, the information is assessed and then system recovery and other recovery actions are performed (e.g., data recovery from backup copies).

Step 7: Initiation of Corrective Actions
The PDBMT identifies and implements corrective actions to avoid repetition of the incident (e.g., addressing vulnerabilities). Indicatively, it may:

- block the attacker from the organisation's network,
- prevent further damage,
- stabilise the affected systems.

Once the data controller has taken all necessary actions to restrain the incident, he/she must proceed with specific actions that will ensure that a similar incident will not re-appear or, if it does, to limit its potential consequences. Thus, the main output of this step is the additional actions that may be enforced by the organisation to prevent the occurrence of similar incidents.

Step 8: Recording personal data breaches
The history of each incident, the accompanying documents, as well as the corrective actions taken, are recorded in the personal data breach archive.

4.3 Fulfilment of Data Subjects' Rights Procedure

Data controllers should follow specific procedures for managing all data subjects' requests related to their rights. Initially, the data controller should identify the data subjects, then evaluate their requests and finally, decide whether to satisfy them or not, informing them accordingly.

4.3.1 Procedure for Fulfilling Data Subjects' Rights
The steps that should be followed to satisfy the data subjects' requests are depicted in Figure 2 and listed next.

Step 1: Collection of data subject's Request
The user (patient) of the RE-SAMPLE platform submits, via the available channels, his/her request regarding his/her personal data, to exercise one of his/her right(s). The supported communication channels that should be available to the data subjects are:

- **Physical Presence**: The data subject fills in a form on the premises of the RE-SAMPLE data controller (see Section 6.5).
- **RE-SAMPLE Website**: The data subject visits the RE-SAMPLE website and completes an online form for exercising his/her rights (see Section 6.5).
- **Mail (physical or electronic)**: The data subject can exercise one of his/her rights by writing free text and sending it to the RE-SAMPLE data controller via physical mail or e-mail.

The process continues with **Step 2**.

Step 2: Data subject's identification and acknowledgement of receipt of her/his request

Upon receiving a data subject's request, the department or individual responsible for handling the request must, within a reasonable timeframe, undertake the process of identifying and authenticating the data subject who submitted the request.

Table 3 outlines the minimum required information for the identification and authentication of the data subject. It's important to note that this set of identification data serves as a baseline, and organisations have the flexibility to use other types of data (e.g., patient ID) for identifying each individual data subject, as long as it meets the necessary criteria for authentication and complies with relevant regulations. This approach allows organisations to tailor their identification methods to their specific needs and circumstances while ensuring data subject rights are respected.

Table 3: Data Subject's Identification Data

Communication channel	Identification data
Physical Presence	Identity card, passport, driving licence
RE-SAMPLE Website	Identification/authentication via the phone.
Mail (Physical or e-mail)	Identification/authentication via the phone.

The department or individual responsible for receiving the request acknowledges its receipt and informs the data subject that the assessment process has been initiated. This acknowledgment is a critical step in effectively monitoring the response timeframe and avoiding unjustified delays in addressing the request.

It is important to emphasize that once the data subject has been successfully identified and authenticated, the data controllers must serve the request and provide a response within 30 days. In exceptional cases where the request is complex or numerous, the organisation may extend this response period by an additional 60 days. However, this extension must be communicated to the data subject along with the reasons for the delay.

In situations where the data controller cannot identify or authenticate a data subject, the request may be rejected. The process then proceeds to **Step 3**, which likely involves further communication with the data subject to resolve any identification or authentication issues. This approach ensures that data subject requests are handled promptly and in compliance with relevant regulations.

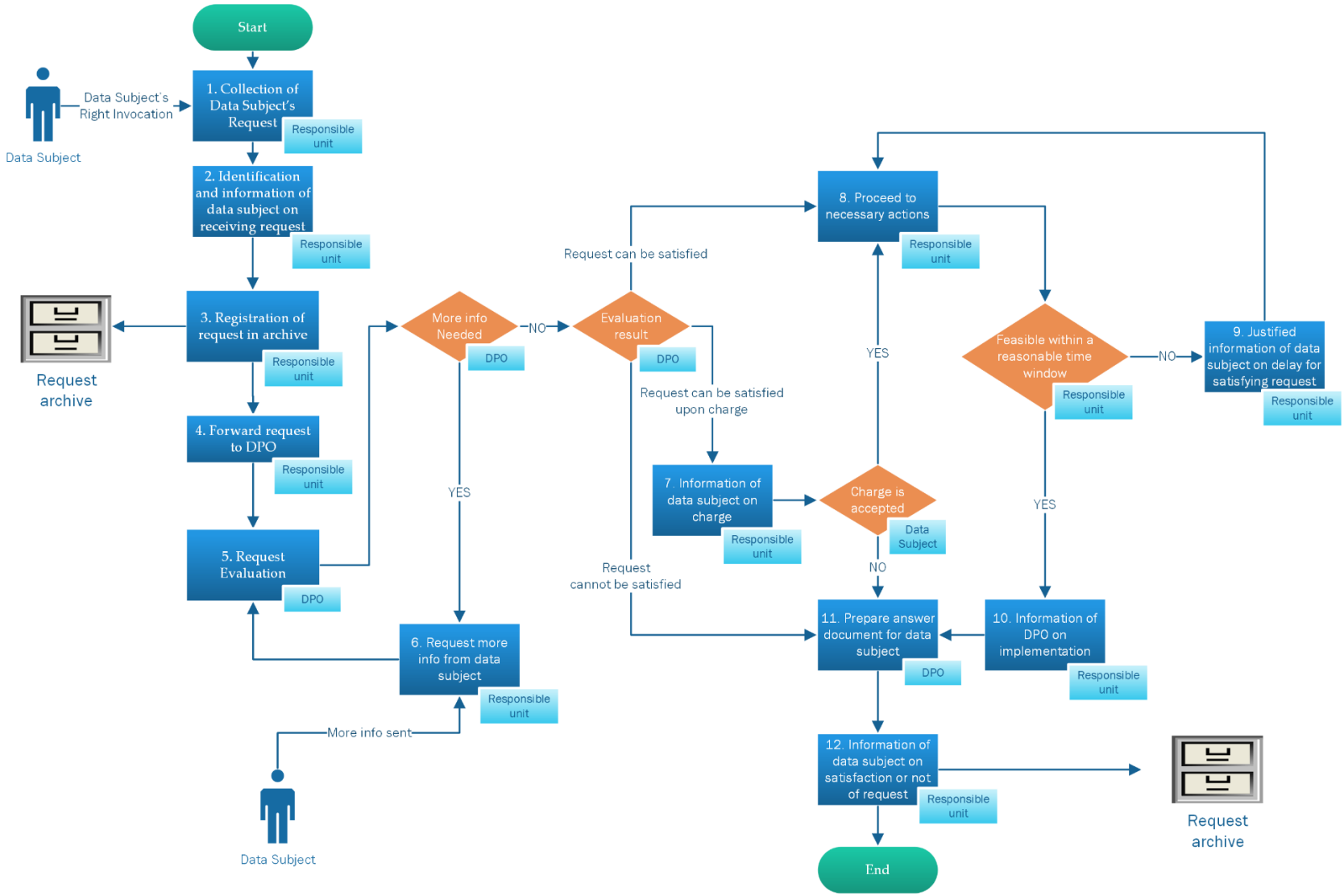

Figure 2: Procedure employed for satisfying RE-SAMPLE data subjects' requests

Step 3: Updating the Request Archive

The department/responsible person who received the request of the data subject registers the request in the "requests archive". In this file (e.g., an Excel file) the RE-SAMPLE data controllers record all the received requests concerning the rights of the data subjects.

For each request, the following information must be recorded:

- **Identification Information:** Unique identification details for the data subject, which may include a patient's unique ID, identity card number, passport number, driving license number, or any other identifiable information that the organisation already utilizes.
- **Type of Exercised Right:** Specify the type of right exercised by the data subject, such as the right of access, right of rectification, right to erasure, etc.
- **Channel of Request Submission:** Indicate the channel through which the data controller received the data subject's request. This could be through an online form, email, postal mail, or another communication method.
- **Preferred Communication Channel:** Record the communication channel through which the data subject wishes to receive the response to their request. For example, the data subject may prefer to receive the response via email or postal mail.
- **Detailed Request Information:** Provide detailed information regarding the specific request made by the data subject. This should include the specific details of the request and any relevant context.
- **Reasons for Assessment Result:** If the data subject's request has been assessed as excessive or lacking appropriate legal basis or grounds, document the reasons that led to this determination.
- **Date of Request Receipt:** Note the date when the request from the data subject was received by the organisation.
- **Date of Data Subject Identification/Authentication:** Record the date on which the data subject was successfully identified and authenticated.
- **Date of Response:** Specify the date on which the data controller provided a response to the data subject's request.
- **Response Channel:** Indicate the communication channel through which the organisation sent the response to the data subject. This could include email, postal mail, or another method.

The "Requests Archive" is updated throughout the execution of the aforementioned procedure. The process continues to **Step 4**.

Step 4: Forwarding the request to the DPO

All requests of the data subjects that were correctly identified in **Step 2**, regardless of the channel through which they were submitted and of the responsible department/person who received them, must be forwarded to the DPO. The procedure continues to **Step 5**.

Step 5: Assessment of the request

The DPO upon receiving a request from a data subject, assumes the responsibility of conducting a thorough assessment of the request. The DPO's role involves analysing the available information to determine whether the request should proceed for satisfaction or if further information from the data subject is required to effectively evaluate the request.

If the available information is considered incomplete and additional information from the data subject is required, the procedure continues to **Step 6**.

Otherwise, if the information is sufficient, he/she can proceed with the assessment of the request. For this assessment, the DPO must seek the necessary information through the available information systems and/or get in touch with the data controller's departments that are related to the request of the data subject.

In addition, the Processing Activities Record, where all personal data processing activities for which the RE-SAMPLE data controller is responsible are recorded, can be used during the assessment of the request since it provides the DPO with important information, including:

- The purpose of processing.
- The potential data recipients (inside and outside the data controller).
- The legal basis of the processing.
- The information systems involved in the processing of the data.

Having this information, the DPO can effectively assess the subject's request and classify it as "a request that can be settled", or a "request that can be settled but a charge is raised for the data subject", or a "request that cannot be settled".

Table 4 provides an indicative guide concerning the assessment of the requests.

Table 4: Data subjects' request assessment table

REQUEST ASSESSMENT TABLE		
Request	**Description**	**Examples of requests**
Request can be settled	Request that can be served within the foreseen timeframe (30 days).	Data rectification Data access Limitation of data processing
Request can be settled but a charge is raised for the data subject	Request that is excessive (e.g., due to its repetitive character).	Multiple copies of data (X times over Y months)
Request cannot be settled	Unjustified request or request that is excessive (e.g., due to its repetitive character).	The data subject requests access to his data, but this will result in the disclosure of personal data of a third party. The data subject has exercised the right to the portability of his/her data but has previously requested the erasure of the data.

If the request is assessed as "request can be settled but a charge is raised for the data subject", the procedure continues to **Step 7**.

If the data subject's request is assessed as "request can be settled", the process continues to **Step 8**.

Finally, if the request is assessed as "request cannot be settled", the procedure continues to **Step 11** of the procedure.

In any case, the DPO informs the responsible departments of the RE-SAMPLE data controller in order to proceed with the necessary actions and / or updates based on the procedure.

Step 6: Requesting additional information from the Data Subject

If the available information when assessing the request is incomplete, then the data controller requests additional information from the data subject. Once the data subject provides the necessary information, the procedure continues to **Step 5** otherwise it stops. The data controller may define a specific timeslot for receiving the additional information requested.

Step 7: Informing the Data Subject of a charge to process the request

The responsible department of the data controller informs the data subject that his/her request will be processed only if they pay a charge corresponding to the complexity of their request. If the data subject accepts the charge, the process continues to **Step 8**. Otherwise, the procedure continues to **Step 11**.

Step 8: Performing the required actions

In order to facilitate communication and interaction with data subjects for the exercise of their rights, the DPO and the RE-SAMPLE data controllers should consider the following options and procedures:

- **Communication Channels:** Data subjects should be offered multiple communication channels to reach out to the data controllers. These channels may include printed or electronic media.
- **Availability of Request Forms:** The form for exercising data subjects' rights (see Section 6.5) should be readily available in both printed form at the data controllers' facilities and in electronic form on the organisation's website. Additionally, an email account can be used by data subjects to submit their requests to the RE-SAMPLE data controllers. During the project, these emails will be received by RE-SAMPLE's DPO. After official deployment, data subjects will contact their respective hospital's DPO.
- **Use of Predefined Templates:** To satisfy the right to information and the right of access, RE-SAMPLE data controllers should utilize predefined templates that are readily accessible to provide clear and standardized responses to data subjects. For the right to information see Section 6.6 and for the right to access see Section 6.7 for the respective templates.
- **Technical Mechanisms:** For rights such as rectification, erasure, objection, limitation of processing, and data portability, data controllers, in collaboration with the DPO, should develop and implement technical mechanisms that support the fulfilment of these rights. These mechanisms ensure that data subjects can effectively exercise these rights.
- **Requests Archive:** Data controllers should maintain a "requests archive" where detailed records of how each data subject's request has been satisfied are documented. This archive ensures transparency, accountability, and compliance with data protection regulations. See Section 6.8 for the respective template.
- **Response Communication:** Data controllers may communicate responses to data subject requests either by letter, either in printed form or electronically. The choice of communication method should consider the data subject's preferences and the options provided during the request submission.

Step 9: Justified information to the Data Subject for delaying the satisfaction of their request

The data controller bears the responsibility of informing the data subject if their request cannot be satisfied within the 30-day timeframe specified by the GDPR. Importantly, this delay must be justified and communicated to the data subject. The justification should outline the reasons for the delay and any relevant factors contributing to the extension of the response time.

The DPO plays a crucial role in overseeing and monitoring the entire process and actions related to the satisfaction of a data subject's request. This continuous monitoring ensures that the request is addressed promptly and in compliance with GDPR requirements. The DPO's involvement helps streamline the process, resolve any potential delays, and maintain transparency in communication with the data subject.

By proactively monitoring the process and taking appropriate actions, the DPO and the data controller work together to ensure that data subject requests are handled efficiently and in accordance with data protection regulations, promoting trust and compliance with the GDPR.

The procedure continues to **Step 8**.

Step 10: Informing the DPO regarding the implementation

The data controller upon completion of all the required actions for the satisfaction of the data subject’s request, must inform the DPO that the request has been served and that no further actions are required. The process continues to **Step 11**.

Step 11: Prepare the response document to the data subject

The DPO has a vital role in thoroughly analysing all available information, regardless of its source, whether it originates from the data subject or arises from the actions of the RE-SAMPLE data controller. The DPO's

responsibilities include preparing the response to the data subject, and these actions are carried out in every case, whether the request is fulfilled or not. The procedure continues to **Step 12**.

Step 12: Informing the data subject regarding the fulfilment or not of the request
The data controller must inform the data subject appropriately for the fulfilment or not of his/her request. Therefore, the response is communicated to the data subject via the selected communication channel. Indicatively:

- Electronically, either if the data subject has requested so or if the request has been submitted by electronic means.
- By letter to the designated postal address of the data subject.
- Orally, if the data subject has requested so.

Finally, the data controller updates the "requests archive". It is noted that this archive proves that the data subject's request has been investigated promptly and the necessary actions have been taken.
The procedure is completed.

4.4 Lawfulness of Processing Procedure

The RE-SAMPLE data controllers should always be able to prove the lawfulness of the processing. The legal basis for the processing of RE-SAMPLE personal data is the **consent** of the data subjects (patients).

4.4.1 Procedure for Obtaining the Data Subjects' Consent

For data controllers to lawfully process personal data, they need the data subjects' consent. If the data subjects are children (below 16 years old), consent must be provided by the holder of parental responsibility. However, the last part is not applicable within the RE-SAMPLE project.

The steps that should follow to obtain the data subjects' consent are shown in Figure 3 and are listed next.

Step 1: Data subjects' Personal Data Fill-in
Data subjects are invited to accept the RE-SAMPLE terms, which should be publicly available on the website (www.re-sample.eu) and easily accessible by the data subjects so that they can either accept them or not, prior to the processing of their personal data. In case of acceptance, the data controller should proceed to Step 2. On the other hand, if the data subject does not accept the terms, he/she cannot be accepted as a RE-SAMPLE user (patient).

Prior to the consent process (Step 2), and more specifically during the enrolment in the RE-SAMPLE system, the patient should be informed (e.g. through a patient information letter) about all essential elements of the processing process, as follows:

- of the identity and contact details of the data controller,
- of the identity and contact details of the DPO,
- of the purposes and legal basis of the processing,
- of the identity and contact details of third parties and recipients potentially involved in data processing,
- of the data retention period,
- of the intention of cross-border transmission,
- of their rights.

The aforementioned information must be in visible form, easily accessible, and understandable so that the data subject has a real choice.

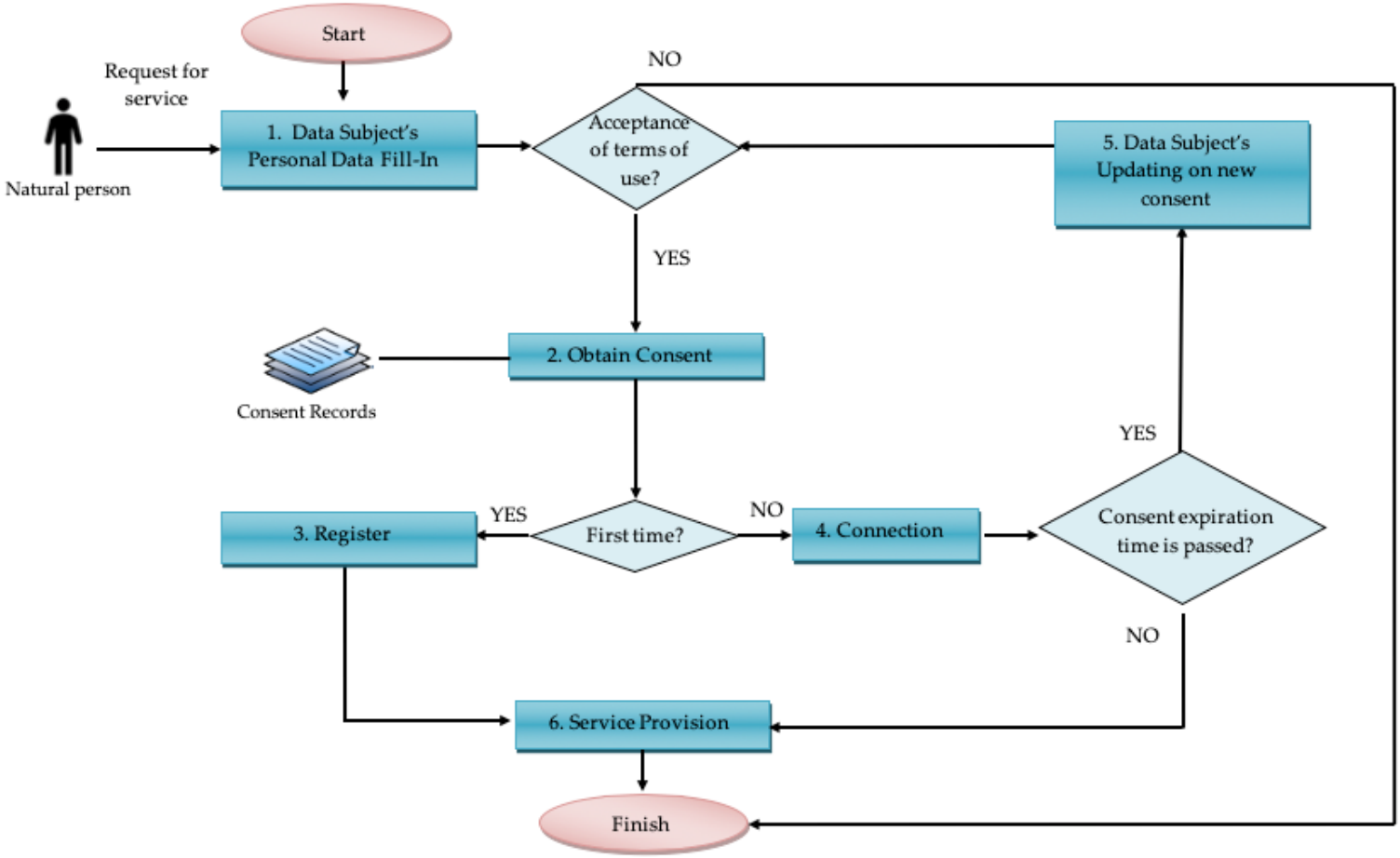

Figure 3: Procedures employed for obtaining the RE-SAMPLE data subjects' consent

Step 2: Obtaining Consent

The RE-SAMPLE data controllers should ensure that a user-friendly consent mechanism is provided (for example through the website or special informed consent forms), so that the patients can clearly express their consent or refusal, regarding the processing of their data. Through these mechanisms, the data controllers must explain the need for data processing (purpose of processing).

If the user (patient) of the RE-SAMPLE platform accepts the RE-SAMPLE terms after being specifically informed (Step 1), then they should provide their consent in order for the data controllers to process their personal data, and in turn, they can use the RE-SAMPLE platform. Table 5 lists alternative ways that the data controllers can enforce to obtain the consent of the data subjects.

Table 5: Alternative Ways for obtaining the consent of data subjects from data controllers

WAYS OF OBTAINING CONSENT	
Means of obtaining consent	**Way of obtaining consent**
Data controller's Website[1]	Digitally signed informed consent
Physical presence	Fill-in and sign a printed copy of the informed consent form (Section 6.2: Consent Form For Using the RE-SAMPLE System and Section 6.1: Consent Form for RE-SAMPLE's Promotion/ Advertising Purposes)

Regardless of the way of obtaining consent, the data controllers must maintain a *Consent Record File* that should include the following:

- identity of the data subjects,
- time that the consent was obtained,
- location and content of consent.

Once the consent process has been completed, if it is the first attempt to access the RE-SAMPLE platform **Step 3** should be followed, otherwise the process continues with **Step 4**.

Step 3: Registration to the RE-SAMPLE platform

If the data subject has consented (**Step 2**) and if it is the first attempt to access the RE-SAMPLE platform (through a healthcare professional), the data subject will be registered.

Step 4: Connection to the system

Once a patient has consented (**Step 2**) and has been registered (**Step 3**), he/she can proceed connecting to the RE-SAMPLE platform (through a healthcare professional). During the connection process, the consent expiration time (if applicable) should be checked. If the determined consent period (if applicable) has not expired, the patient may continue using RE-SAMPLE. Otherwise, the procedure continues to **Step 5**. In any case, the patient has the right to request withdrawal of his/her consent by filling out the template form of Section 6.3.

Step 5: Renewing the data subject's consent

If the data subject's consent period has expired (if applicable) he/she must be informed accordingly. In this case, the RE-SAMPLE terms should be re-accepted for the patient to be allowed to continue using the RE-SAMPLE platform. If he/she accepts the terms of use, the process continues to **Step 2**.

Step 6: Service Provision

Once the above steps of the process are completed, the patients have the right to use the RE-SAMPLE platform.

[1] Or other Information System accessible via a website in general.

4.5 Personnel Training Procedures

The primary focus of this training is to prevent errors that may result in personal data breaches, enable early detection of incidents, and ensure the implementation of appropriate countermeasures. While dedicated training may not be necessary for RE-SAMPLE, the suggested activities below should be followed by clinical partners to effectively implement the privacy policy. Training is particularly important for IT staff, informing them about new threats, risks, and security measures. Training should be conducted regularly, such as at least every 6 months, and should include the following steps:

Step 1: Knowledge and skills requirements definition
Data controllers' technical personnel should be aware of the current data protection policy. Additionally, they must develop skills on technical countermeasures (hardware, applications, software tools).

Step 2: Training groups' separation (if any)
Where necessary, the personnel will be divided in different groups. The criteria may be: a) past assessments and performance differentiation, b) years of service, c) specialised knowledge required by particular people.

Step 3: Designing training plan and evaluation methods
In this step the training and evaluation plan is designed, which includes at least the following elements:

- Training subjects and content (e.g. training on Intrusion Detection Systems)
- Matching of training content to the required knowledge and skills
- Training tools (e.g. webinars, e-learning, lectures)
- Metrics and evaluation tools (e.g. tests, simulations)

Step 4: Training implementation
In this step the training is implemented according to the training plan.

Step 5: Training evaluation
In this step the evaluation of the training is performed in order to assess the ability of the personnel to apply current technical countermeasures to the protection of the RE-SAMPLE platform, the knowledge acquired on personal data protection and the compliance with the GDPR, and in general on the level of assimilation of the content of the training.

4.6 Personnel Awareness Procedure

Raising awareness among personnel about privacy issues is crucial, especially when handling personal and sensitive information like users' personal data and health data. It's an ongoing process that requires careful planning and execution. Here are the essential steps for ensuring personnel awareness on privacy issues:

Step 1: Awareness target(s) identification and groups' separation (if any)
Dividing personnel into groups for tailored privacy awareness training is a practical and effective approach, considering that different roles and experience levels within an organisation may require specific training. Here's how you can categorize personnel into groups for customized sensitizing needs in data privacy issues:

1. **Role-Based Groups:** Organize personnel into groups based on their specific roles and responsibilities within the organisation. This can include categories such as:

    - **Data Handlers:** Those who directly handle or process personal data.
    - **IT Staff:** IT professionals responsible for data security and system management.
    - **Healthcare Professionals:** Medical staff who interact with patient health data.
    - **Administrative Staff:** Personnel who handle administrative and non-clinical data.
    - **Management and Decision-Makers:** Executives and managers with decision-making authority regarding data privacy.

2. **Experience-Based Groups:** Consider dividing personnel based on their years of service or experience in data privacy matters. This ensures that both newcomers and existing staff receive training that aligns with their knowledge and awareness levels. Groups might include:

    - **New Hires:** Employees who have recently joined the organisation and need fundamental privacy training.
    - **Experienced Staff:** Personnel who have been with the organisation for an extended period and may require more advanced or specialized training.

3. **Data Sensitivity Groups:** Group personnel based on the sensitivity of the data they handle. For example:

    - **Highly Sensitive Data Handlers:** Employees who work with extremely sensitive personal or health data.
    - **Moderately Sensitive Data Handlers:** Those who manage less sensitive personal data.
    - **Non-Sensitive Data Handlers:** Personnel dealing with non-sensitive or administrative data.

4. **Data Subject Interaction Groups:** Consider the level of interaction personnel have with data subjects:

    - **Frontline Staff:** Those who directly interact with data subjects, such as healthcare providers.
    - **Back-Office Staff:** Employees who work behind the scenes and may not have direct data subject contact.

5. **Compliance and Legal Teams:** Personnel responsible for ensuring the organisation's compliance with data protection regulations may require specialized training tailored to their legal and regulatory responsibilities.

6. **Technical vs. Non-Technical:** Distinguish between technical and non-technical roles, as the training needs and content may differ significantly. Technical staff may need more in-depth knowledge about security measures and technology-related risks.

Step 2: Designing a privacy awareness plan

Designing an effective awareness program for data privacy and protection is essential for ensuring that personnel are well-informed and vigilant about privacy issues. Here are the key elements to include in your awareness program:

- **Thematic Sections:** Your awareness program should cover a range of thematic sections to provide comprehensive knowledge about data privacy and protection. Consider including, at a minimum, the following topics:

    - **GDPR Basics:** Explain the fundamental concepts of the GDPR, including the definition of personal data, the identification of data processing purposes, and an overview of data subject rights.
    - **RE-SAMPLE's Data Protection Policy:** Familiarize personnel with the organisation's data protection policy, including its purpose and key working practices.
    - **User Account Protection:** Educate employees on the importance of securing their user accounts, including best practices for creating strong passwords and safeguarding login credentials.
    - **Social Engineering and Phishing:** Raise awareness about social engineering tactics, spam emails, electronic phishing, and fraud schemes. Teach personnel how to recognize and respond to phishing attempts.

    - **Malware and Virus Protection:** Provide guidance on protecting against malware and viruses, including safe browsing habits, downloading practices, and the use of antivirus software.
    - **Physical Security:** Discuss the importance of physical security measures, such as securing physical documents, locking devices, and preventing unauthorized access to sensitive areas.

- **Communication Channels:** Choose communication channels that best suit the size and preferences of your personnel. Consider a mix of the following channels:

    - **Training Sessions:** Conduct in-person or virtual training sessions to deliver detailed information on each thematic section. These sessions allow for interactive discussions and Q&A sessions.
    - **Social Media:** Utilize social media platforms to share brief tips, articles, and infographics on data privacy topics. Social media can facilitate ongoing engagement and reminders.
    - **Promotional Tools:** Create promotional items with messages about personal data protection, such as posters, brochures, and office signage. These serve as visual reminders in the workplace.
    - **Newsletters:** Publish regular newsletters that include articles, case studies, and updates related to data privacy and protection. Newsletters can reach a wide audience and keep personnel informed.
    - **Events:** Organize events, workshops, or webinars dedicated to data privacy topics. These events provide an opportunity for interactive learning and discussion.

- **Regular Updates:** Ensure that your awareness program is not a one-time effort but an ongoing process. Regularly update and refresh the content to address emerging threats and changes in regulations.

- **Assessment and Feedback:** Include mechanisms for assessing personnel's understanding of data privacy concepts. Encourage employees to provide feedback on the awareness program to make continuous improvements.

- **Management Support:** Secure the support of senior management to emphasize the importance of data privacy and protection. Their endorsement can reinforce the significance of the program.

- **Customization:** Tailor the program to the specific needs and roles of different employee groups within the organisation. Consider their level of interaction with personal data and their job responsibilities.

- **Compliance Emphasis:** Highlight the legal and regulatory aspects of data protection, emphasizing the consequences of non-compliance.

Step 3: Implementing data protection awareness actions

In this step, the awareness raining actions are implemented.

Step 4: Awareness program assessment

The implementation of awareness raising actions is an on-going process in order to bring long-term results. However, it is advisable to regularly assess the impact of the awareness program (e.g. annually) on the personnel. The assessment can be implemented with predefined metrics such as the number of participants in program events, the number of incidents of data disclosure as a result of human failure, performance in assessment exercises, etc.

4.7 Transferring Processing Activities to Data Processors

If a RE-SAMPLE data controller, needs to assign a processing activity (that includes processing of personal data) to other parties, which will act as data processors, he must ensure that the other party will sign an agreement that will include at least the following:

- Purpose of processing
- Exact way and terms of processing of the personal data by the data processor
- Procedure for acquiring and storing personal data by the data processor
- Data processor's right to perform personal data transmission, to communicate with the data subjects and to handle data subjects' requests according to their rights.
- Rules for the protection of personal data
- Other obligations – Data processor's rights

In the context of RE-SAMPLE the data controllers (clinical partners) have already signed Data Processing Agreements with other project partners (technical partners) for the scope of the project and got aware of the steps that need to be followed for accomplishing this procedure.

4.8 Guidelines for Processing Personal Data for Research Purposes

This section provides guidance on the obligations of the data controller when processing personal data in the context of scientific research, ensuring compliance with GDPR provisions before, during, and after the research.

The following guidelines should be followed by anyone intending to carry out scientific research that includes the collection and processing of personal data. The guidelines consist of nine (9) steps that must be performed before the research starts.

Step 1: Determine the purpose or purposes of processing

Initially, the researcher(s) must identify and determine the purpose (or purposes) of data processing in the context of the scientific research. As it is often quite difficult to identify this from the very beginning, the researcher must, at least, describe in a higher level the purpose of the research.

Step 2: Ability to use anonymized data during the research

The researcher should assess whether it is necessary to have access to the identities of individuals participating in the scientific research. If the research can be conducted using anonymized data, this approach should be adopted.

Anonymized data refers to information that cannot be associated with any participant in the research, making it impossible for the researcher, any collaborators, or third parties with data access to identify an individual. It's important to note that processing anonymized data falls outside the scope of GDPR, relieving the researcher of the need to follow the remaining steps outlined in this section.

Step 3: Determining the legal basis

According to the GDPR, in order for a personal data processing to be lawful it must fall under one of the legal bases of Article 6.1. More specifically, data can be processed for research purposes when:

- The subject has given his/her consent
- The subject has already consented to the reuse of his/her data, or to use it for similar purposes, in previous research
- The personal data concerning the subject come from a publicly accessible source
- Processing is necessary for the research and the researcher can prove that the purposes of the scientific research do not outweigh the interests and rights of the data subjects.

However, it is important to note that using the consent of the subjects as the legal basis of the processing is not the best choice, as the research may be harmed or even stopped if the data subjects decide to withdraw their consent.

When special categories of personal data are processed (Articles 9 and 10 of the GDPR), the purpose of the research conducted based on the personal data used should also consider the respective risk raised for potential privacy violations. Thus, the purpose of the research should be proportionate to the additional risks imposed.

Step 4: Ensuring proper guarantees.

Processing personal data for research purposes must be accompanied by suitable safeguards to uphold the rights and freedoms of the individuals involved, as stipulated by GDPR. These safeguards are designed to ascertain that the researcher has put in place the necessary technical and organisational measures.

However, in order to use personal data for research purposes, the principle of "*data minimization*" must be ensured. More precisely, the researcher should take care of the following:

1. **What personal data is really needed?**

The researcher should gather and handle data that is pertinent and essential to the particular objectives of the scientific study. Moreover, prior to data collection, the researcher should evaluate the nature and objectives of the research to determine whether broader information or specific data is required. For instance, if the research can be adequately conducted using only the participants' year of birth or age, there is no need for precise birthdates.

2. **The ability to pseudonymize data**

The researcher ought to employ measures that encompass pseudonyms (pseudonymization) if the research permits such an approach. Pseudonyms must be stored separately from the personal data, either in physical or electronic form, with access restricted solely to authorized members of the research team. This practice serves to reduce the potential risks of data exposure or the identification of participating individuals by external collaborators or unauthorized parties who lack access to the personal data file.

3. **Who will have access to the data**

The data controller should guarantee that access to participants' personal data and their pseudonyms is limited to individuals who have a legitimate need to know. For example, in many instances, only a subset of the research team requires knowledge of participant identities to carry out the research. Therefore, personal data should only be shared with third parties essential for conducting the research.

Step 5: Identifying the involved third parties

All third parties who are involved must be identified before initiating the scientific research. More specifically:

- In case both the purpose and the way of conducting the scientific research are determined by one organisation then this organisation acts as the Data Controller.
- In case the purpose and/or the way of conducting the research are determined by several collaborating parties, then all of them act as Joint Data Controllers.
- In case the collaborating parties process participants' personal data under the guidance of the Data Controller, then the collaborating parties act as Data Processors. In addition, anyone else (natural or legal person) who processes personal data on behalf of the Data Controller acts as a Data Processor.

In each of the aforementioned scenarios, whenever data is shared or processed by third parties participating in the research, the data controller should insist that the collaborating party enters into a contract. This contract will outline the responsibilities of the collaborating third party, whether they are jointly responsible for processing or conducting the processing itself, concerning the protection of personal data. In this regard,

the principal investigator should consult the DPO when considering collaboration with a third party to ensure that it meets the necessary criteria for data protection.

Step 6: Decision to conduct a Data Protection Impact Assessment

Prior to commencing the research, the research team members should evaluate whether the processing of personal data could potentially present a significant risk to the rights and freedoms of the individuals involved. Specifically, the research team members should ascertain whether the processing falls under the DPA's list of processing activities that necessitate a DPIA. If the processing is not mentioned in the provided list, the principal investigator should then determine whether it meets any of the following criteria:

- Evaluation or grading or profiling, among others, of individuals
- Automated decision-making, that produces legal effects for the individual
- Processing "prevents data subjects from exercising a right or using a service or contract"
- Systematic monitoring of data subjects, including network monitoring and "systematic monitoring of publicly accessible space"
- Processing of special categories of personal data (Article 9 GDPR) and / or personal data related to criminal convictions or offenses (Article 10 GDPR)
- Processing of data concerning vulnerable individuals, such as children, employees, people with disabilities, etc.
- Match or combine two or more different data sets
- Large-scale processing of personal data
- Innovative use or application of new technological or organisational solutions, such as the "Internet of Things" (IOT), biometric technologies, etc.

If the type of processing is in the DPA list or at least two of the above criteria are met, the DPIA is required.

Step 7: Implementation of additional technical and organisational measures

It is crucial for the data controller to ensure that personal data used for the research is handled securely throughout its lifecycle, including collection, storage, transmission, and eventual destruction. In this regard, the research team of the data controller implements the necessary technical and organisational measures as required. These measures may be necessary either due to the identification of risks in the DPIA that need mitigation or as part of general data protection measures.

In particular, in order to protect the rights and individual liberties of the subjects, but also the personal data related to them, from unauthorized access/use, unauthorized modification, accidental (or not) loss, destruction or damage, a range of technical and organisational protection measures (Table 6) should be applied.

Table 6: Indicative protection measures

INDICATIVE TECHNICAL AND ORGANIZATIONAL MEASURES
ORGANIZATIONAL MEASURES
- Design and implementation of a framework regarding the protection of personal data (policies, procedures, guidelines) regarding: o the basic principles governing the processing of personal data o managing the requests of the subjects regarding their rights o obtaining and managing the consent of the subjects o the maintenance of a processing activities archive o conducting an impact assessment on data protection o the transmission of data to countries outside the EU o data protection by design and by default o reporting and dealing with personal data breaches, etc.
- Determining the time of retaining personal data and implementing a procedure for their secure deletion, both in paper and electronic form.
- Determining the legal basis of processing operations.

INDICATIVE TECHNICAL AND ORGANIZATIONAL MEASURES
- Check the necessity of the personal data collected through electronic forms, applications or other forms of the data controller.
- Development of material and implementation of training and awareness programs concerning the protection of personal data.
- Implement a procedure regarding the management of information security risks.
- Implement a framework for the classification of information (e.g. internal use, confidential, classify).
- Restriction of access to personal data based on roles and responsibilities.
- Implement a strict password policy.
TECHNICAL MEASURES
- Mechanisms related to the fulfilment of legal obligations of the data controller, such as application for the handling of requests and consents of subjects.
- Mechanisms for assigning a specific retention period to data (e.g. via metadata) and automatically deleting them when the retention period has expired.
- Control of logical access to folders, files, databases, systems, applications that contain personal data.
- Data verification and user authorization mechanisms.
- Mechanisms to prevent identification of the data subject (e.g. anonymization, pseudonymization, masking).
- Encryption of personal data stored in systems / databases of the Data Controller, especially if they belong to a special category.
- Encryption of digital communication channels in order to securely transmit personal data.
- Logging activity on systems.
- Back up data.
- Storage of personal data only in cloud computing that provides an acceptable level of protection and has been approved by the data controller.
- Secure storage of documents in physical form (e.g. fire safe areas, restricted areas)
- Control of physical access to the premises where personal data are kept (e.g. secured premises and doors, escort of visitors)

The researcher in charge should seek guidance from the DPO and/or relevant departments within the data controller regarding the protective measures they need or want to implement. For instance, the researcher may consult with the IT Department for advice on approved services for storing and transmitting personal data, as well as assistance with access rights and encryption. Furthermore, if the researcher requires a secure physical location for storing hard-copy documents, they can get in touch with the data controller's administration, responsible for document management.

Step 8: Creation of an information sheet regarding the processing of personal data and declaration of consent

After completing the above steps, the researcher has to provide a document describing the processing carried out in the context of the research. The information sheet should ensure that data subjects have received all the necessary information regarding the processing of their data. In Table 7 the information that has to be communicated to the data subjects according to the GDPR (Articles 13 and 14), depending on whether their personal data have been collected directly by researcher or not, is presented.

Table 7: Information Sheet context

What the information sheet should include:	When data is collected directly by the subject	When data is not collected directly by the subject
The identity and contact details of the data controller and DPO.	✓	✓
The processing activity and its legal basis.	✓	✓

What the information sheet should include:	When data is collected directly by the subject	When data is <u>not</u> collected directly by the subject
The purpose or purposes of processing.	✓	✓
The categories of personal data.		✓
The recipients or the categories of recipients of the personal data, if any.	✓	✓
Information regarding the transmission of data to a third country and the appropriate guarantees, if any.	✓	✓
The period for which the personal data will be stored or the criteria that determine it.	✓	✓
Information regarding the rights of the subject according to the GDPR.	✓	✓
Information regarding the existence of the right of revoking the consent, if any.	✓	✓
Information regarding the existence of the right to file a complaint to the supervisory authority.	✓	✓
The source of the personal data and whether the data derives from publicly accessible sources.		✓
The existence of automated decision making, including profiling.	✓	✓

Furthermore, information regarding the processing of personal data should adhere to international standards. It should encompass general details about the scientific research, such as its title, duration, and subject. It should also provide clarifications about potential risks or benefits associated with the research. Additionally, it must clearly state that participation is entirely voluntary, and participants have the right to withdraw from the research at any time without any negative consequences.

If the processing relies on the consent of the participants, the researcher should also create a consent statement that aligns with GDPR requirements and official standards for scientific research.

<u>Step 9: Scientific publications of research results</u>

If researchers intend to publish their findings, which may include personal data of the participants, they must obtain explicit consent from the data subjects. To address this, it is recommended that researchers consider presenting and publishing, whenever feasible, an anonymized version of the research report.

5. Conclusions

The primary objective of deliverable D4.8, entitled "Security and Data Protection Policies," within *Task 4.5 "Security & privacy measures, security & data protection policies"* under Work Package 4 (WP4), was to create the security and data protection policy for the RE-SAMPLE platform. To achieve this, Section 3 initially provided a high-level overview of the general data protection rules, followed by the specific Data Protection Policy tailored to the RE-SAMPLE platform as presented in Section 4. Finally, in Section 6 a set of template forms is presented for assisting RE-SAMPLE data controllers to apply the data protection policy.

This deliverable has one more iteration at the end of the project where the updates from the application of the policy to the clinical partners (data controllers) will be addressed concluding the organisational and procedural measures along with the technical security and privacy requirements addressed in the respective deliverables of WP4.

6. Appendix

6.1 Consent Form for RE-SAMPLE's Promotion/ Advertising Purposes

Conference/Workshop/Meeting …
(Title of event)
Date ___ /___ / ____

RE-SAMPLE Data Controllers respect personal data and comply with the requirements set by the General Data Protection Regulation (GDPR) and other laws or/and codes of conduct. To this respect, the participants of the conference/workshop/meeting are asked to decide if they agree with the processing of their personal data (the ones presented in the following table are only indicative, every Data Controller should alter these fields based on their privacy policy) for the purposes listed next.

PERSONAL DATA[2]:

First Name:	Last Name:	
Father's Name:	Mother's Name:	Date of Birth:

CONTACT ADDRESS:

Street:	Number:
City:	Postal code:
Phone Number:	Mobile Phone Number:
E-mail:	

- ☐ "I give my consent to the RE-SAMPLE Data Controller to send me material for this event"
- ☐ "I give my consent to the RE-SAMPLE Data Controller to send me relevant informational material, such as brochures and newsletters"
- ☐ "I am aware of the video/photographs taken during this event and I give my consent to the RE-SAMPLE Data Controller to process (i.e. collect, store and use) photos and videos in which I appear, or audio taken during this event according to its dissemination plan/strategy for promotion and advertising purposes. RE-SAMPLE Data Controllers may transfer or give access to data to another company"

In order to withdraw your consent to the processing of your personal data, or to exercise any of your rights (access, rectification, erasure, object, portability, restriction of processing), you may contact …….. at …….. In any case, you have the right to file a complaint to the Data Protection Authority.

Name/Surname: …… **Date: ……**
E-mail: …….. **Signature: ……**

[2] The following personal data is listed indicatively and RE-SAMPLE Data Controllers should collect ONLY the ones necessary for the Purpose of Processing.

6.2 Consent Form For Using the RE-SAMPLE System

Protocol Number: _____*
Date: _____*
*Filled in by the Organisation

Addressed to the RE-SAMPLE Data Controller _____,

Participation in the RE-SAMPLE System

RE-SAMPLE Data Controller respects personal data and comply with the requirements set by the General Data Protection Regulation (GDPR) and other laws or/and codes of conduct. To this respect, you are asked to decide if you agree with the processing of your personal data (the ones listed below) for serving the following RE-SAMPLE's purposes of processing:

1. "Design, implement and evaluate the VCP to support patients with COPD and CCC and the HCPs that treat them"

RE-SAMPLE's goal is to use Real World Data to improve the healthcare journey of patients with Chronic Obstructive Pulmonary Disease (COPD) and comorbidities, and to set a standard of care for patients suffering from Complex Chronic Conditions (CCCs). The data and analyses will serve as a basis for predictive models that will help patients and their healthcare professionals (HCPs) make treatment and lifestyle changes in time to reduce complications.
The aforementioned "Purpose of Processing" serves RE-SAMPLE's main goal to identify individual multi-morbid CCC exacerbations and develop tailored referral to a multidisciplinary, adaptive Virtual Companionship Programme (VCP) for patients with COPD and CCCs.

For satisfying the specific purpose of processing the data will be collected - processed:

a. **Sensor data** from sensors, which are mainly connected to the Healthentia Platform, e.g.,:
    i. physiological data (heart rate data, sleep data, daily physiological data and daily activity data).
b. **questionnaire data,** which are collected through the answers given by the patients to questionnaires asked through the Healthentia Platform, and can be further divided into:
    i. Daily data (daily symptom diary data COPD and CCC)
    ii. Exacerbation data, obtained if symptoms are increased (e.g., quality of life, reason for exacerbations)
    iii. Usability data
c. **Health Information System (HIS) data**, composed of information acquired from the HIS and grouped into:
    i. Follow-Up data: information obtained by the HCPs during the baseline and the follow-up visits at the clinical sites where several procedures are carried out:
        - Spirometry (regular or after bronchodilators treatment)
        - Six-minute walking test
        - Blood test
        - Medications administered
        - Clinical outcomes
    ii. Hospitalization data: information retrieved by the HCPs whenever a patient is hospitalized.
d. **Machine Learning (ML) Data t**hat are generated by the ML modules and comprise predictions, explanations, and simulations. These predictions reflect whether the patient's health condition is worsening or not.

2. "Anonymization of patients' data and provision of the anonymized data, in the form of Open Data, for medical-scientific research purposes

The Hospital may decide to anonymize part or all patients' data and offer them, in the form of Open Data, to third parties for medical-scientific research purposes. For safeguarding the patients' privacy rights, access to the anonymized data will be granted after an access request of the interested party and only for the aforementioned purpose(s) of processing. This also applies to researchers (Ph.D. students – Postdocs) working in RE-SAMPLE, provided that their research is compatible with the aforementioned purposes of processing and that the Hospital approves the access request. The request should at least include an analysis plan describing: 1) study objective and outcome parameters, 2) choice of population(s), 3) sample size, 4) choice of requested data, 5) working plan, 6) authorship.

For satisfying this/these purpose(s) of processing no more personal data will be collected. Instead, the RE-SAMPLE Data Controller will anonymize the data already collected, as well as the data produced from the processing of the original data, and will offer them, in the form of Open Data, to third parties upon approval from the Hospital.

Furthermore, the RE-SAMPLE Data Controller informs you about the following:

1. You have the right to submit a request to the RE-SAMPLE Data Controller exercising your rights (access, rectification, erasure, restriction of processing, objection, data portability).
2. You have the right to withdraw your consent.
3. You have the right to file a complaint to the Data Protection Authority of your country.
4. The RE-SAMPLE controller will not use the data collected for purposes other than those specified above.
5. The personal data collected by the RE-SAMPLE Data Controller will not be transferred or/and accessed by any external entity/organization, **with the following exceptions**:
   a. **For the first purpose of processing**:
      i. If the patient agrees (as part of the shared decision making) a coaching strategy will be transferred to Healthentia and will be utilized by the Healthentia Dialogue System as input to coach and support the patient in disease management.
      ii. To facilitate automatic medication suggestions (based on the symptom diary linked to the action plan) the medication prescriptions that the patient has will be transferred to Healthentia.
   b. **For the second purpose of processing**: Data may be anonymized and offered to third parties for research purposes as explained above.
6. Regarding the automated decision-making and profiling, RE-SAMPLE Data Controllers commit not to use the personal data for automated decisions or profiling purposes.
7. The patients will always have the ability to delete their data by notifying the RE-SAMPLE Data Controller. The deletion process will permanently delete all patients' data except data stored in anonymised form for research purposes. Data will be stored for all the period that the patient uses the RE-SAMPLE services.

PATIENT's PERSONAL DATA[3]:

First Name:	Last Name:	Job Description:
Father's Name:	Mother's Name:	Date of Birth:

PATIENT's CONTACT ADDRESS:

Street:	Number:
City:	Postal code:
Phone Number:	Mobile Phone Number:
E-mail:	

[3] The following personal data is listed indicatively and RE-SAMPLE Data Controllers should collect ONLY the ones necessary for the Purpose of Processing.

☐ I hereby declare that having been informed about the processing of my personal data related to the RE-SAMPLE's purpose of processing:

"Design, implement and evaluate the VCP to support patients with COPD and CCC and the HCPs that treat them"

I give my consent to the processing of my personal data.

☐ I hereby declare that having been informed about the processing of my personal data related to the RE-SAMPLE's purpose of processing:

"Anonymization of patients' data and provision of the anonymized data, in the form of Open Data, for medical-scientific research purposes

I give my consent to the processing of my personal data.

In order to withdraw your consent to the processing of your personal data, or to exercise any of your rights (access, rectification, erasure, object, portability, restriction of processing), you may contact …….. at ……. . In any case, you have the right to file a complaint to the Data Protection Authority.

Name/Surname: ……
E-mail: ……..

Date: ……
Signature: ……

6.3 Data Subject's withdrawal of consent

Protocol Number: _____*
Date: _____*
*Filled in by the Organisation

Addressed to the RE-SAMPLE Data Controller _____,

Data Subject's PERSONAL DATA[4]:

First Name:	Last Name:	
Father's Name:	Mother's Name:	Date of Birth:

CONTACT ADDRESS:

Street:	Number:
City:	Postal code:
Phone Number:	Mobile Phone Number:
E-mail:	

Declaration:
I attach the necessary identification documents and I request **withdrawal** of my consent regarding the collection and processing of my personal data for the following processing activities (purpose of processing):

- ☐ "Design, implement and evaluate the VCP to support patients with COPD and CCC and the HCPs that treat them"
- ☐ "Sending promotional/advertising material for RE-SAMPLE events"
- ☐ "Sending RE-SAMPLE informational material (e.g. brochures, newsletters etc.)

I responsibly certify the accuracy and correctness of those written above.

Number of attached files: _____

Name/Surname: ……
E-mail: ……..

Date: ……
Signature: ……

[4] The following personal data is listed indicatively and RE-SAMPLE Data Controllers should collect ONLY the ones necessary for identifying the data subject.

6.4 Notification of Personal Data Breach

Protocol Number: _____
Date: _____
Incident Number: _____

REPORT OF PERSONAL DATA BREACH		
First Name:	Last Name:	Title/Status: (*user, anonymous, employee*)
Phone Number:	Mobile Phone Number:	email:
Street:		Number:
City:		Postal code:

INFORMATION ABOUT THE INCIDENT			
CATEGORISATION OF THE INCIDENT:	• Maximum Priority • Medium Priority • Minimum Priority	DATE OF INCIDENT:	
LOCATION			
CITY:		COUNTRY	POSTAL CODE:
SPECIFIC LOCATION (if there is any):			
SHORT REPORT OF THE INCIDENT: General Information: ● Data Volume: _____ ● Source of Data Breach: _____ ● Why is the Data in danger: _____ ● Is the Data Encrypted: _____			
Type of Data			
• Names • Codes / passwords • E-mail Addresses • Text in e-mails • Phone Numbers • Addresses • Identification Number / Passport Number		• Medical Data • Other sensitive Personal Data _____ _____ • Other sensitive information _____ _____	
Type of Incident			
- Network or Server Breach - Loss or steal or infringement of a computer in which data is stored - Malicious Software		- Unauthorised access - Other _____ _____	
CAUSES OF THE INCIDENT:			
CONSEQUENSES OF THE INCIDENT:			

CORRECTIVE ACTIONS:
CONCLUSIONS – FURTHER OBSERVATIONS:

Name/Surname: ……..…
E-mail: ……..

Date: ……
Signature: ……

6.5 Form for exercising Data Subject's Rights

(Provided by the RE-SAMPLE Data Controllers to the Data Subjects, filled in by the Data Subject and addressed to the RE-SAMPLE Data Controller)

Data Subject's Request (Exercising Data Subject's Rights)

Protocol Number: _____*
Date: _____*
*Filled in by the Organisation

Addressed to the RE-SAMPLE Data Controller _____,

In order to exercise your rights, you can contact the RE-SAMPLE Data Controller through:

Mail	
Phone	
Fax	
E-mail	

Data Subject's PERSONAL DATA[5]:

First Name:	Last Name:	
Father's Name:	Mother's Name:	Date of Birth:

CONTACT ADDRESS:

Street:	Number:
City:	Postal code:
Phone Number:	Mobile Phone Number:
E-mail:	

I request to exercise my right to[6]:

- ☐ Information
- ☐ Access
- ☐ Rectification
- ☐ Erasure
- ☐ Object
- ☐ Restriction of Processing
- ☐ Data Portability

It is noted that exercising your rights does not raise any charge for you (except for cases with repetitive character or for cases requiring excessive work; in all these cases the data subjects will be informed prior to the processing of their request).
The RE-SAMPLE Data Controllers will fulfil the data subject's request within one month. If the actions necessary for fulfilling the request are demanding and complicated, RE-SAMPLE Data Controllers have the right to extend the

[5] The following personal data is listed indicatively and RE-SAMPLE Data Controllers should collect ONLY the ones necessary for identifying the data subject.
[6] In order to exercise the right to rectification, erasure, objection, restriction of processing and data portability, the Data Subject must attach the necessary additional information.

above period of time for two more months. In that case you will be informed within a month from the date that you submitted the request.

Name/Surname: ……
E-mail: ……..

Date: ……
Signature: ……

6.6 Response to Request for Information

(Filled in by the RE-SAMPLE Data Controller and addressed to the Data Subject)

Protocol Number: _____*

Date: _____*

*Filled in by the Organisation

Addressed to the Data Subject _____

Controller			
Name of RE-SAMPLE Data Controller			
Contact Information			
Data Protection Officer			
First Name/Last Name			
Contact Information			
Purpose of processing			
Data Collected / Processed		**Purpose of Processing**	
Legal Basis of Processing/Lawfulness of processing			
Legitimate interests pursued by RE-SAMPLE Data Controllers			
Recipients of Personal data			
Intention to deliver data to third countries or International Organisations			
Period of time that the personal data will be stored			

6.7 Response to the exercise of the right of access

(Filled in by the RE-SAMPLE Data Controller and addressed to the Data Subject)

Protocol Number: _____*
Date: _____*
*Filled in by the Organisation

Addressed to the Data Subject _____

Purpose of processing
Categories of personal data stored / processed
Recipients of Personal Data
Period of time that the personal data will be stored [7]

[7] When it's impossible to define the specific period of time, RE-SAMPLE controllers mention the criteria which determine that period of time.

6.8 Management Request

RE-SAMPLE Data Controllers maintain a "Requests Archive" where details of how each data subject's request has been satisfied can be found. To this direction, RE-SAMPLE controllers could use the following template.

INFORMATION ON THE SUBMISSION OF THE REQUEST

Date of Receipt: ……
Unit: ……
Received by: ……

Actions of the Unit

INFORMATION ON THE PROCESSING OF THE REQUEST

Unit: ……
Processed by: ……
Signature: ……
Date: ……

Actions of the Unit