iProcureSecurity PCP

Pre-Commercial Procurement
of Innovative Triage Management Systems
Strengthening Resilience and Interoperability
of Emergency Medical Services

D1.2 Data Management Plan

Project

Acronym	**iProcureSecurity PCP**
Title	Pre-Commercial Procurement of Innovative Triage Management Systems Strengthening Resilience and Interoperability of Emergency Medical Services
Coordinator	SYNYO GmbH
Reference	101022061
Type	Pre-commercial procurement (PCP)
Programme	HORIZON 2020
Topic	H2020-SU-SEC-2020
Start	01.09.2021
Duration	36 months
Website	https://pcp.iprocuresecurity.eu/
Consortium	**SYNYO GMBH** (SYNYO), Austria **EMPRESA PUBLICA DE EMERGENCIAS SANITARIAS** (EPES), Spain **SERVICIO MADRILENO DE SALUD** (SERMAS), Spain **OSTERREICHISCHES ROTES KREUZ** (ARC), Austria **AZIENDA SANITARIA LOCALE BENEVENTO** (ASLBN), Italy **AGENZIA REGIONALE EMERGENZA URGENZA** (AREU), Italy **ELLINIKOS ERYTHROS STAVROS** (HRC), Greece **ETHNIKO KENTRO AMESIS VOITHEIAS** (EKAB), Greece **IZMIR BUYUKSEHIR BELEDIYESI** (IBB), Turkey **KENTRO MELETON ASFALEIAS** (KEMEA), Greece **ACIL AFET AMBULANS HEKIMLERI DERNEGI** (AAHD), Turkey **EMPIRICA GESELLSCHAFT FUR KOMMUNIKATIONS- UND TECHNOLOGIEFORSCHUNG GMBH** (EMPIRICA), Germany

Acknowledgement: This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 101022061.

Deliverable

Number	**D1.2**
Title	**Data Management Plan**
Lead beneficiary	KEMEA
Work package	WP1
Dissemination level	Public (PU)
Nature	Open Research Data Pilot (ORDP)
Due date	31.01.2022
Submission date	24.02.2022
Authors	**Panagiota Benekou, KEMEA** **Georgia Melenikou, KEMEA**
Contributors	**All Partners**
Reviewers	**Alberto Lombardi, ASLBN** **Serena Bianchi, SYNYO** **Bernhard Jäger, SYNYO**

Document history

Version	Date	Comments
0.1	15/12/2021	Skeleton
0.2	10/01/2022	First draft
0.3	25/01/2022	Incorporation of partners' input
0.4	31/01/2022	Final draft - Ready for review
0.5	3/02/2022	Partner information update
0.6	7/02/2022	Review by ASLBN
0.7	8/2/2022	Information update based on review
0.8	10/2/2022	Additional Partner information update
0.9	14/2/2022	Additional updates
1.0	24/02/2022	Submission (SYNYO)

Executive Summary

This deliverable constitutes the Data Management Plan (DMP) of the iProcureSecurity PCP project, outlining the main elements of the data management policy that will be used by the whole consortium. The DMP gives a general outline of the rights and the integrity of all generated/processed/collected data as well as the procedures that will be followed to acquire the data with respect to their sensitiveness and the measures that need to be followed throughout this process. In that way, the DMP presents how research data will be handled during the project, and even after the project is completed, describes what data, methodology and standards will be followed, whether this data will be shared and/or made open.

The described data management policy reflects the current state of consortium agreements regarding data management and is consistent with those referring to exploitation and protection of results and can also be considered as a checklist for the future. Moreover, the different aspects of making data Findable, Accessible, Interoperable and Re-usable (FAIR) are presented as well as the security, ethical and privacy-related aspects.

Contents

Tables

1 Introduction

Emergency Medical Services (EMS) in Europe are characterized by a heterogeneous landscape with diverse organizational setups, technology standards, coordination mechanisms and actors. This is the result of different historical and institutional contexts. However, these EMS are united by the common aim of providing timely care to victims of sudden and life-threatening emergencies or disasters in cross-border settings and international humanitarian missions. Fostering the response capacities and increasing the cooperation of the Emergency Medical Services Systems (EMSS) is of decisive importance for strengthening the resilience of European societies.

During the prior iProcureSecurity project, a large number of EMS were involved to identify, evaluate and prioritize future challenges and needs. The creation of an interoperable, flexible triage management system supported by modern technologies was among the most requested solutions in the context of security-related scenarios.

This iProcureSecurity PCP action is a result of those intense participatory consultation processes. The action will lead to an innovative triage management system that provides a) quick and accurate overview of victims and their status; b) decision support for better allocation of available resources and quicker support for patients; c) improved interoperability with other first responders and relevant actors; d) reduced handover times between ambulance transport and hospitals; and e) insights for quality assurance and training measures.

Following the EC Guidelines on Pre-Commercial Procurement (PCP), through a competitive series of design, prototype and pilot steps, the iProcureSecurity PCP will contract suppliers to deliver the creation and deployment of the envisaged triage management system.

Besides the buyers within the consortium, additional observers and experts will participate to contribute to the Pan-European improvement in this field and to proactively share PCP knowledge.

1.1 Purpose of the Document

This document provides an analysis of the main elements of the data management policy that will be used by iProcureSecurity PCP project consortium with regards to all the datasets that will be generated by the project during its implementation. It describes the data management life-cycle for all data sets that will be collected, processed or generated by the research project. It is a document outlining how research data will be handled during a research project, and even after the project is completed, describing what data will be collected, processed, or generated and following what methodology and standards, whether and how this data will be shared and/or made open, and how it will be curated and preserved.

The DMP is a living document updated and reviewed according to the project developments and the Horizon 2020 guidelines. The second updated version will be submitted as a deliverable in Month 12 (D1.5) and the final version will be updated and submitted in Month 36 (D1.6).

1.2 Definitions, Acronyms and Abbreviation

Table 1: **Definitions and Acronyms**

Acronym	Definition
D	Deliverable
DMP	Data Management Plan
DPO	Data Protection Officer
EC	European Commission
EU	European Union
GDPR	General Data Protection Regulation
IP	Intellectual Property
IPR	Intellectual Property Rights
PCP	Pre-commercial Procurement
WP	Work Package

2 Data Management Plan

2.1 Data Summary

2.1.1 Purpose of the data collection/generation and its relation to the objectives of the project

iProcureSecurity PCP challenge is to develop an interoperable, flexible triage management system supported by modern technologies able to provide a) quick and accurate overview of victims and their status; b) decision support for better allocation of available resources and quicker support for patients; c) improved interoperability with other first responders and relevant actors; d) reduced handover times between ambulance transport and hospitals; and e) insights for quality assurance and training measures.

2.1.2 Data to be collected/ generated

The data to be collected generated can be grouped in the following categories:

Information about the consortium: Data about the consortium, such as personal information, emails etc. will be handled and stored in a private and secure repository accessed only by the members of the consortium.

Project files: Data gathered from meetings, workshops, and any type of internal communication will be protected according to each required level of confidentially. Fruitful and general outcomes of the project will be disseminated without restriction if no sensitive data are disclosed. In the case of

confidential discussions or outcomes (e.g. EU Restricted deliverables), only specific partners will have access

Research activities: In the case of research that involves collection of data, such data will be stored and protected locally by the corresponding organization. Proper organisational and technical measures including these of anonymization and/or encryption mechanisms will be applied to protect the rights and freedoms of the data subjects.

Pilots: Information regarding the persons involved in pilots and the processed data will be stored and managed by Buyers' Group and potentially by the Contractors. The outcomes of such testing will be reported in an anonymized form.

Since this is an early stage, a second version (D1.5) is foreseen to be added as a deliverable in Month 12 of the project in order to give a clearer and complete overview of the generated and used data and cover any gaps that exist in the present. A final updated version (D1.6) will follow in Month 36.

2.1.3 Types and formats of data that the project will collect/ generate per partner

In order to fulfil the aforementioned purpose, iProcureSecurity PCP project will collect and generate the following data:

Table 2: **Data to be collected and generated**

Data / Data Sources	Type	Data Format		Data Origin				
			Consortium Meetings	Interviews, UOG	Questionnaires	Testing	Deliverables Preparation	Literature Review
			All WP	WP2	WP2	WP6,7,8	All WPs	All WPs
Literature	Electronic document	Word (.doc/.docx) Pdf					✓	✓
	Paper document						✓	✓
References	Electronic document	Endnote database (.enl) Word (.doc/.docx)					✓	✓
	Paper Document						✓	✓
Consent Form	Paper Document (signed)		✓	✓	✓	✓	✓	
Questionnaires	Electronic document	Word (.doc/.docx) Excel (.xls/.xlsx) Pdf	✓	✓	✓	✓	✓	

	Paper Document		✓	✓	✓	✓	✓	
Images	Electronic Document	TIFF, JPEG, PNG, JPEG/JFIF, GIF etc.	✓	✓	✓	✓		
	Paper Document		✓	✓	✓	✓		
Audio Files	Electronic Document	WAVE, AIFF, MP3, MXF, FLAC etc.	✓	✓	✓	✓		
Video Files	Electronic Document	MOV, MPEG-4, AVI, MXF etc.	✓	✓	✓	✓		
Deliverable	Electronic Document	Word (.doc/.docx) Excel (.xls/.xlsx) Pdf	✓	✓	✓	✓	✓	✓
	Paper Document		✓	✓	✓	✓	✓	✓
Software	Code	Several Programme Languages					✓	
Software Data	Database	Database Management System				✓	✓	

Additionally, the following tables present partners' input regarding to the data that will be collected and generated per partner for the iProcureSecurity PCP project.

SYNYO GmbH

Table 3: **SYNYO DMP Questionnaire**

Data Description	
What type of data will you collect? Please provide in brief.	Publicly available data on: - organisations (research, industry, procurers) - experts - projects - solutions - events Collection of current status of triage management, requirements, use cases and processes (this data is collected by procurer partners, the collection process is guided by SYNYO). SYNYO receives only aggregated data from the partners which does not contain personal information.
What is the purpose of the data collection?	Reaching out to relevant organizations, experts, projects, events to raise awareness on the project and important activities (e.g. Open Market Consultations) Information on available solutions will be checked during the analysis of requirements and use cases.
Please explain: • What is the origin of the data? • Are you using data someone else produced? If so, where is it from?	Publicly available data or Primary data, questionnaires filled out by the suppliers, procurers, expert and advisory board members and observer group members. Personal data will be collected from the data subjects themselves. Aggregated data on current status of triage management and requirement, use cases and processes provided by procurement partners.
What types of data do you expect to be processed / generated? Please refer to both	Data to be processed: a) personal data (names, contact details, images, voices) of participants in

special categories of personal data and non-special categories.	the OMC events, b) information of state of art technologies through OMC questionnaires, c) data of contractors as part of the procurement process.
Please explain the relation of the data processing/generation (for each data type) to the objectives of the project.	The collected data is needed to prepare the call for tender (specification of the required solution) and for outreach activities to ensure all target groups are addresses appropriately and can participate in and benefit from the project and its outcomes. The data will be used for the purpose of the project only.
How will you be processing the data? Provide separate answers for each data type/category you will be processing, collecting, or generating.	The collected data will be used to approach relevant organizations and experts. The provided information from the procurers on their current triage management status, requirements, use cases and process models will be used by SYNYO (jointly with all partners) to establish clear specifics to be used in the tender documents.
For each data type, please state the format(s) in which you expect that type of data to be collected/generated. For example, numerical data, image data, text sequences, audio data etc.	The collected data (all types mentioned above) will be mainly stored in spreadsheets (e.g. xlsx). Videos (e.g. of OMCs) will be captured as mp4 or similar video codecs. Reporting of project activities will take place in Microsoft Word (.docx) and submitted as pdf to the Funding Authority.
For each type of data what is the expected size?	<1MB (all except video) <500MB (video)

Data Management Procedures	
Does your organization have data management guidelines? If so, what are they?	SYNYO follows EC's relevant guidelines.
Does your organization have a data protection or security policy that you will follow? If so, what is it?	Yes, has a Data Protection Policy.
Does your organization have a Research Data Management policy? What is it?	According to the DMP
Are there any formal standards you will adopt when processing data for the project?	According to SYNYO's data protection policy.
Please provide the contact details of your organization's DPO.	SYNYO has not designated a Data Protection Officer and is not required to do so according to article 37 par. 1 GDPR.

Documentation, Organization and Storage	
Who will be responsible for documentation, organization, and storage?	Project Manager

How will you label and organize data, records, and files?	All data will be labelled with the project acronym and a unique name and version number (where necessary).
How long will you be storing personal data generated in the project for?	For 5 years after the end of the project.
How and where will the data be stored?	Internal policies, confidentiality agreements, secured storage of documents where only authorized access is allowed, using data-protection focused service providers and storage platforms, controlled password-protected access to personal computers and to databases, privacy by design techniques, encrypted file transfers, anonymization, pseudonymization
Are you using proprietary file formats to generate and store your research data? If so, will the documentation about the software needed to access the data be included?	Yes, xls.
If data are collected with mobile devices, how will you transfer and store the data?	N/A
If data are held in various places, how will you keep track of versions?	N/A

Access	
Who within your organization will manage access to this data?	Project Manager
Who within your organization will have access to the data processed for the iProcureSecurity PCP project?	Project Manager
How will the identity of the person accessing the data be ascertained?	Password protection
Will there by conditions to gaining data access? If so, what will those conditions be?	N/A
What methods or software tools will be needed to access the data? Will any other accompanying information be required to properly interpret the data?	Microsoft Office No
What information, if any needs to be retained in order for the data to be read and interpreted in the future?	N/A
Will any data be made openly available for all project partners?	Project partners will have access and contribute to all types of collected data mentioned above.
How will the data that is made openly available be maintained? In a repository?	GDPR compliant collaboration software

Sharing	
What data will be shared?	As mentioned above.
When will data be shared?	During the project lifetime

For what purposes of the project will data be shared?	Awareness for the project activities (e.g. OMCs, call for tender, observer and expert board) and retrieving expert opinion and feedback (e.g. from Ethics Advisor).
Who will data be shared with?	Project partners, Ethics Advisor.
Does sharing raise any privacy, ethical, or confidentiality concerns? If yes, what are they and why?	No
Will a data sharing agreement be required? If some data categories and types are kept closed provide a rationale for doing so.	No

Security	
What are the major risks to data security?	Major risks: Viruses, Data phishing, Data loss, Data breach (confidentiality, availability). However, majority of collected data is publicly available or will be made public (e.g. through public Deliverables).
How will each of these risks be managed?	N/A
Do you need to anonymize any of the data?	N/A
What security measures do you anticipate being required for safe data storage, sharing and management?	Internal policies, confidentiality agreements, secured storage of documents where only authorized access is allowed, using data-protection focused service providers and storage platforms, controlled password-protected access to personal computers and to databases, privacy by design techniques, encrypted file transfers, anonymization, pseudonymization
Have you implemented or outlined any procedures to follow in the case of a data breach? If so, what are they?	According to GDPR Art. 33, 34
Are your digital and non-digital data, and any copies, held in a safe and secure location?	Yes

Ethical Considerations	
What types of special category personal data do you intend to generate/process?	Voice of partners/participants in recorded webinar
Will any of the data subjects be children?	No
Will any of the data subjects be vulnerable people?	No
Will you be collecting personal or sensitive data from people who have not given their explicit consent to participate in the Project?	No
For each category of data you intend to collect, please provide:	• Art. 6 par. 1(a) consent (from webinar and interviews participants and for partners' images and voice)

• If the data is personal data, as defined by the GDPR, which of the six Art. 6 bases will you rely on for the processing of each category of personal data? • If the data is sensitive data, as defined by the GDPR, which of the ten Art. 9 bases will you rely on for the processing of each category of sensitive data?	• Art. 6 par. 1(b) contract (for partners' names and contact details) • Art. 9 par. 2 (a) consent (for webinar participants' voice).
Have you already gained consent for data preservation and sharing from any data subject(s)?	Yes, for the following activities: - Subscription to the project newsletter - Pre-registration/registration to project related events - Participation in project boards Furthermore, SYNYO provided all partners collecting information during Interviews/Workshops/Focus Groups with an Informed Consent sheet template
Will you engage in large scale or big data processing?	No
Will any entity (including any service provider) outside of the E.U. have access to personal or sensitive data? If so, who? For what purpose? Where is each of these entities located?	No personal data or sensitive data is shared. Project partners located in Turkey (AAHD, IBB) for the sole purpose to fulfil project tasks (such as awareness raising for project activities, collect information on current state of triage management, identify requirements, use cases and processes).

EMPRESA PUBLICA DE EMERGENCIAS SANITARIAS, EPES

Table 4: **EPES DMP Questionnaire**

Data Description	
What type of data will you collect? Please provide in brief.	No personal data has been collected, only the data of the persons involved in the project.
What is the purpose of the data collection?	Facilitate health care in multiple accidents, leaving a register of all those data that, under medical criteria, allow for accurate and updated knowledge of the state of health.
Please explain: 1. What is the origin of the data?	Health care for health problems in an out-of-hospital setting.

• Are you using data someone else produced? If so, where is it from?	
What types of data do you expect to be processed / generated? Please refer to both special categories of personal data and non-special categories.	No personal data is being processed.
Please explain the relation of the data processing/generation (for each data type) to the objectives of the project.	No personal data is being processed.
How will you be processing the data? Provide separate answers for each data type/category you will be processing, collecting, or generating.	The collected data will be collected in the Digital Mobility Health Record and sent to the Referral Hospital to which the patients will be referred to prepare for care
For each data type, please state the format(s) in which you expect that type of data to be collected/generated. For example, numerical data, image data, text sequences, audio data etc.	It depends. Most probably, numerical data, image data, text sequences and audio data.
For each type of data what is the expected size?	Unknown at this stage.

Data Management Procedures	
Does your organization have data management guidelines? If so, what are they?	The company has documentation and procedures related to the management of personal data.
Does your organization have a data protection or security policy that you will follow? If so, what is it?	Our organisation has procedures, protocols and guidelines for data protection.
Does your organization have a Research Data Management policy? What is it?	We comply with GDPR and national laws
Are there any formal standards you will adopt when processing data for the project?	Yes, there are some formal standards. In our organisation, data collection and consent forms are available.
Please provide the contact details of your organization's DPO.	DPD: Juan Dïaz García spd.sspa@juntadeandalucia.es

Documentation, Organization and Storage	
Who will be responsible for documentation, organization, and storage?	The Head of Information Security together with the Director of Technological Processes
How will you label and organize data, records, and files?	Following standard procedures for the data protection of clinical information
How long will you be storing personal data generated in the project for?	5 years after the end of the project.
How and where will the data be stored?	It will be stored in the repository of the project
Are you using proprietary file formats to generate and store your research data? If so, will the	We will be using the Microsoft and Drive formats

documentation about the software needed to access the data be included?	
If data are collected with mobile devices, how will you transfer and store the data?	No data will be collected using mobile devices
If data are held in various places, how will you keep track of versions?	It only will be stored in the repository of the project

Access	
Who within your organization will manage access to this data?	Information Security Manager
Who within your organization will have access to the data processed for the iProcureSecurity PCP project?	The professionals involved in the project
How will the identity of the person accessing the data be ascertained?	The identity procedures are the ones applied to access the mail account s/he is registered with
Will there by conditions to gaining data access? If so, what will those conditions be?	A data access protocol will be established by means of approvals.
What methods or software tools will be needed to access the data? Will any other accompanying information be required to properly interpret the data?	The reports can be accessed using only the edition tolls of the said repository
What information, if any needs to be retained in order for the data to be read and interpreted in the future?	The tools used are standard
Will any data be made openly available for all project partners?	All data is available to all the project partners
How will the data that is made openly available be maintained? In a repository?	It will be maintained in the common repository

Sharing	
What data will be shared?	Project-related data
When will data be shared?	As soon as it is produced
For what purposes of the project will data be shared?	For all the purposes of the project as are agreed in the GA and during the execution of the project among the partners
Who will data be shared with?	The partners of this project
Does sharing raise any privacy, ethical, or confidentiality concerns? If yes, what are they and why?	No
Will a data sharing agreement be required? If some data categories and types are kept closed provide a rationale for doing so.	There should be a confidentiality agreement between all parties.

Security	
What are the major risks to data security?	The same risks as the access to the organization systems.

How will each of these risks be managed?	The Centro de Emergencias Sanitarias 061 has its own safety procedures.
Do you need to anonymize any of the data?	No
What security measures do you anticipate being required for safe data storage, sharing and management?	No extra measures. The system is well protected
Have you implemented or outlined any procedures to follow in the case of a data breach? If so, what are they?	The procedures established by GDPR
Are your digital and non-digital data, and any copies, held in a safe and secure location?	All data are in the repository of the project

Ethical Considerations	
What types of special category personal data do you intend to generate/process?	No personal data will be generated
Will any of the data subjects be children?	No personal data will be generated
Will any of the data subjects be vulnerable people?	No personal data will be generated
Will you be collecting personal or sensitive data from people who have not given their explicit consent to participate in the Project?	No personal data will be generated
For each category of data you intend to collect, please provide: 2. If the data is personal data, as defined by the GDPR, which of the six Art. 6 bases will you rely on for the processing of each category of personal data? • If the data is sensitive data, as defined by the GDPR, which of the ten Art. 9 bases will you rely on for the processing of each category of sensitive data?	No personal data will be generated
Have you already gained consent for data preservation and sharing from any data subject(s)?	No personal data will be generated
Will you engage in large scale or big data processing?	No
Will any entity (including any service provider) outside of the E.U. have access to personal or sensitive data? If so, who? For what purpose? Where is each of these entities located?	No personal data will be generated

SERVICIO MADRILENO DE SALUD, SERMAS

Table 5: **SERMAS DMP Questionnaire**

Data Description	
What type of data will you collect? Please provide in brief.	Until now we have collected no personal data apart from the contact data of the persons who work in the project, and no other personal data is envisaged to be neither collected nor stored. The data we manage are the public documents that are generated during the project.
What is the purpose of the data collection?	The purpose of the data stored is the correct execution of this project
Please explain: • What is the origin of the data? • Are you using data someone else produced? If so, where is it from?	We produce the data that is stored in the shared documents stored in the project repository
What types of data do you expect to be processed / generated? Please refer to both special categories of personal data and non-special categories.	No personal data is being processed.
Please explain the relation of the data processing/generation (for each data type) to the objectives of the project.	No personal data is being processed.
How will you be processing the data? Provide separate answers for each data type/category you will be processing, collecting, or generating.	No personal data is being processed.
For each data type, please state the format(s) in which you expect that type of data to be collected/generated. For example, numerical data, image data, text sequences, audio data etc.	No personal data is being processed. In any case we only generate and contribute only text reports
For each type of data what is the expected size?	Some megabytes of text data

Data Management Procedures	
Does your organization have data management guidelines? If so, what are they?	We comply with GDPR and national laws
Does your organization have a data protection or security policy that you will follow? If so, what is it?	Only GDPR compliance
Does your organization have a Research Data Management policy? What is it?	It is not applicable to this project
Are there any formal standards you will adopt when processing data for the project?	No, there are not
Please provide the contact details of your organization's DPO.	delegadodatosfibhnjs@salud.madrid.org

Documentation, Organization and Storage	
Who will be responsible for documentation, organization, and storage?	FIIBAP Director
How will you label and organize data, records, and files?	We tag the reports with the prefix iProcureSecurity PCP
How long will you be storing personal data generated in the project for?	Just until two years after the end of the project
How and where will the data be stored?	It will be stored in the repository of the project
Are you using proprietary file formats to generate and store your research data? If so, will the documentation about the software needed to access the data be included?	We will be using the Microsoft and Drive formats widely used
If data are collected with mobile devices, how will you transfer and store the data?	No data will be collected using mobile devices
If data are held in various places, how will you keep track of versions?	It only will be stored in the repository of the project

Access	
Who within your organization will manage access to this data?	The registered users of the repository of the project
Who within your organization will have access to the data processed for the iProcureSecurity PCP project?	The registered users of the repository of the project
How will the identity of the person accessing the data be ascertained?	The identity procedures are the ones applied to access the mail account s/he is registered with
Will there by conditions to gaining data access? If so, what will those conditions be?	No more conditions will be asked for
What methods or software tools will be needed to access the data? Will any other accompanying information be required to properly interpret the data?	The reports can be accessed using only the edition tolls of the said repository
What information, if any needs to be retained in order for the data to be read and interpreted in the future?	The tools used are standard
Will any data be made openly available for all project partners?	All data is available to all the project partners
How will the data that is made openly available be maintained? In a repository?	It will be maintained in the common repository

Sharing	
What data will be shared?	Reports and collaborators contacts
When will data be shared?	As soon as it is produced
For what purposes of the project will data be shared?	For all the purposes of the project as are agreed in the GA and during the execution of the project among the partners
Who will data be shared with?	The partners of this project

Does sharing raise any privacy, ethical, or confidentiality concerns? If yes, what are they and why?	No concerns are envisaged
Will a data sharing agreement be required? If some data categories and types are kept closed provide a rationale for doing so.	Only the CA

Security	
What are the major risks to data security?	The same risks as the access to the organization systems
How will each of these risks be managed?	The organization has its own security procedures
Do you need to anonymize any of the data?	No
What security measures do you anticipate being required for safe data storage, sharing and management?	No extra measures
Have you implemented or outlined any procedures to follow in the case of a data breach? If so, what are they?	The procedures established by GDPR
Are your digital and non-digital data, and any copies, held in a safe and secure location?	All data are in the repository of the project

Ethical Considerations	
What types of special category personal data do you intend to generate/process?	No personal data will be generated
Will any of the data subjects be children?	No personal data will be generated
Will any of the data subjects be vulnerable people?	No personal data will be generated
Will you be collecting personal or sensitive data from people who have not given their explicit consent to participate in the Project?	No personal data will be collected
For each category of data you intend to collect, please provide: • If the data is personal data, as defined by the GDPR, which of the six Art. 6 bases will you rely on for the processing of each category of personal data? • If the data is sensitive data, as defined by the GDPR, which of the ten Art. 9 bases will you rely on for the processing of each category of sensitive data?	No personal data will be collected
Have you already gained consent for data preservation and sharing from any data subject(s)?	No personal data will be collected
Will you engage in large scale or big data processing?	No

Will any entity (including any service provider) outside of the E.U. have access to personal or sensitive data? If so, who? For what purpose? Where is each of these entities located?	No personal data will be collected

OSTERREICHISCHES ROTES KREUZ, ARC

Table 6: **ARC DMP Questionnaire**

Data Description	
What type of data will you collect? Please provide in brief.	End user requirements in the means of specifications, desired features, usability and performance among others. No personal data will be collected.
What is the purpose of the data collection?	Identifying user needs for developing products according to user specifications
Please explain: • What is the origin of the data? • Are you using data someone else produced? If so, where is it from?	• Focus groups and interviews with practitioners and experts. • All data is collected inside the organization, thus no external data is used.
What types of data do you expect to be processed / generated? Please refer to both special categories of personal data and non-special categories.	• specifications • desired features • usability and • performance among No personal data is being or will be processed.
Please explain the relation of the data processing/generation (for each data type) to the objectives of the project.	Data is needed to design the procurement according to end user needs
How will you be processing the data? Provide separate answers for each data type/category you will be processing, collecting, or generating.	No personal data is being or will be processed. Raw data is given to the coordinator/WP leader who is in charge of to process it
For each data type, please state the format(s) in which you expect that type of data to be collected/generated. For example, numerical data, image data, text sequences, audio data etc.	No personal data is being or will be processed. If some, then text data
For each type of data what is the expected size?	<1MB

Data Management Procedures	
Does your organization have data management guidelines? If so, what are they?	The following legal provisions are relevant for data protection: Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27th 2016 for the protection of natural persons when processing personal Data, the free movement of data and the repeal of Directive 95/46 / EC (General Data Protection Regulation, GDPR) Data Protection Amendment Act 2018 as amended
Does your organization have a data protection or security policy that you will follow? If so, what is it?	GDPR
Does your organization have a Research Data Management policy? What is it?	It is not applicable to this project.
Are there any formal standards you will adopt when processing data for the project?	No
Please provide the contact details of your organization's DPO.	MAG. SANDRA SCHINNER Management 1/Data Protection Department Austrian Red Cross, Headquarters Wiedner Hauptstraße 32, 1040 Wien, Österreich E: sandra.schinner@roteskreuz.at

Documentation, Organization and Storage	
Who will be responsible for documentation, organization, and storage?	Project managers/assistant of Department: Operations/National disaster management & Research
How will you label and organize data, records, and files?	Reports are tagged with prefix [iProcureSecurity PCP]
How long will you be storing personal data generated in the project for?	For the duration of the project
How and where will the data be stored?	It will be stored in the repository of the project /Drive, ARC's Sharepoint
Are you using proprietary file formats to generate and store your research data? If so, will the documentation about the software needed to access the data be included?	ARC will be using the Microsoft and Drive formats (widely used)
If data are collected with mobile devices, how will you transfer and store the data?	No data will be collected using mobile devices. No data will be transferred or stored by using mobile devices.
If data are held in various places, how will you keep track of versions?	It only will be stored in the repository of the project.

Access	
Who within your organization will manage access to this data?	Only registered users of the repository of the project – Department responsible for the project: Operations and National disaster management and Research
Who within your organization will have access to the data processed for the iProcureSecurity PCP project?	Only department responsible for the project: Operations and National disaster management and Research
How will the identity of the person accessing the data be ascertained?	The identity procedures are the ones applied to access the mail account s/he is registered with
Will there by conditions to gaining data access? If so, what will those conditions be?	No more conditions will be asked for.
What methods or software tools will be needed to access the data? Will any other accompanying information be required to properly interpret the data?	The reports can be accessed using only the edition tolls of the said repository
What information, if any needs to be retained in order for the data to be read and interpreted in the future?	The tools used are standard.
Will any data be made openly available for all project partners?	All data is available to all project partners.
How will the data that is made openly available be maintained? In a repository?	Right, in a repository.

Sharing	
What data will be shared?	Interviews and focus group discussion as outcomes
When will data be shared?	As soon as it is produced.
For what purposes of the project will data be shared?	For all purposes of proper project management such agreed in the GA and during the execution of the project among the partners
Who will data be shared with?	Project consortium.
Does sharing raise any privacy, ethical, or confidentiality concerns? If yes, what are they and why?	No concerns are envisaged.
Will a data sharing agreement be required? If some data categories and types are kept closed provide a rationale for doing so.	CA

Security	
What are the major risks to data security?	The same risks as the access to the organization systems.
How will each of these risks be managed?	The Austrian Red Cross has its own security procedures.
Do you need to anonymize any of the data?	no

What security measures do you anticipate being required for safe data storage, sharing and management?	Any extra measures, the system is well protected.
Have you implemented or outlined any procedures to follow in the case of a data breach? If so, what are they?	We implemented all the procedures established by GDPR.
Are your digital and non-digital data, and any copies, held in a safe and secure location?	All data are in the repository of the project.

Ethical Considerations	
What types of special category personal data do you intend to generate/process?	No personal data will be generated or processed.
Will any of the data subjects be children?	no
Will any of the data subjects be vulnerable people?	no
Will you be collecting personal or sensitive data from people who have not given their explicit consent to participate in the Project?	no
For each category of data you intend to collect, please provide: • If the data is personal data, as defined by the GDPR, which of the six Art. 6 bases will you rely on for the processing of each category of personal data? • If the data is sensitive data, as defined by the GDPR, which of the ten Art. 9 bases will you rely on for the processing of each category of sensitive data?	No personal data will be collected.
Have you already gained consent for data preservation and sharing from any data subject(s)?	No personal data will be collected.
Will you engage in large scale or big data processing?	No
Will any entity (including any service provider) outside of the E.U. have access to personal or sensitive data? If so, who? For what purpose? Where is each of these entities located?	No personal data will be collected.

AZIENDA SANITARIA LOCALE BENEVENTO, ASLBN

Table 7: **ASLBN DMP Questionnaire**

Data Description	

<table>
<tr><td>What type of data will you collect? Please provide in brief.</td><td>In the PHASE 0 -PHASE 1 – PHASE 2
Types of personal data that we collect and process:
- Personal Identification Data.
- Surveys and personal interviews
- Notes, audio and/or video recordings of your activities that may be made during Co-creative workshops and multidisciplinary focus groups.
- Additional information that you provide may be used in the dissemination and promotion of iProcureSecurity PCP in general.

No other use will be made of them without your written permission
In the PHASE 3
- possibility of using health and sensitive data for the cluster of users participating in the field test
-

<table><tr><th>n.</th><th>DATA SETS</th></tr><tr><td>1</td><td>Stakeholders contact collection</td></tr><tr><td>2</td><td>State-of-the-art overview collection</td></tr><tr><td>3</td><td>Market solutions overview</td></tr><tr><td>4</td><td>Demand-side and supply-side questionnaires</td></tr><tr><td>5</td><td>Expert interview data</td></tr><tr><td>6</td><td>Focus groups data</td></tr><tr><td>7</td><td>OMC Workshops data</td></tr><tr><td>8</td><td>OMC Webinar data</td></tr><tr><td>9</td><td>Matchmaking platform</td></tr><tr><td>10</td><td>PCP Challenge brief</td></tr><tr><td>11</td><td>Call for tender applicants’ data</td></tr><tr><td>12</td><td>Call for tender documentation (Prior Information notice; tender specifications, tender criteria, etc.)</td></tr><tr><td>13</td><td>Framework Agreement</td></tr><tr><td>14</td><td>Specific Phase contracts</td></tr><tr><td>15</td><td>User’s Prototype data</td></tr><tr><td>16</td><td>Stakeholder’s Prototype data</td></tr><tr><td>17</td><td>Field-testing data</td></tr><tr><td>18</td><td>Impact assessment evaluation</td></tr></table></td></tr>
<tr><td>What is the purpose of the data collection?</td><td>The iProcureSecurity PCP Consortium is committed to protect personal data and to respect data subject’s privacy. Our Partners' lawful bases for processing personal data, as set out in Article 6 of the GDPR, vary depending on</td></tr>
</table>

<table>
<tr>
<td></td>
<td>the particular processed personal data whose they refer with.

The participation in the study is completely voluntary.

The data collection is related to

- Co-creative workshops to stimulate new ideas.
- Surveys and personal interviews to assess the needs and possible innovations.
- Multidisciplinary focus groups for needs analysis.

The main purpose of the evaluation is to gather information about expert opinion regarding the shortcomings of the medical emergency system, the possibilities of improvement through innovation and to gather the requirements for the prototypes.

The information collected in the study will be anonymised and the personal data stored in an encrypted way.

Personal data will not be used for any automated decision-making including profiling.</td>
</tr>
<tr>
<td>Please explain:
• What is the origin of the data?
• Are you using data someone else produced? If so, where is it from?</td>
<td>
<table>
<tr><th>n.</th><th>DATA SETS</th><th>ORIGIN</th></tr>
<tr><td>1</td><td>Stakeholders contact collection</td><td>Publicly available data</td></tr>
<tr><td>2</td><td>State-of-the-art overview collection</td><td>Publicly available data</td></tr>
<tr><td>3</td><td>Market solutions overview</td><td>Publicly available data</td></tr>
<tr><td>4</td><td>Demand-side and supply-side questionnaires</td><td>Primary data</td></tr>
<tr><td>5</td><td>Expert interview data</td><td>Primary / personal data</td></tr>
<tr><td>6</td><td>Focus groups data</td><td>Primary data</td></tr>
<tr><td>7</td><td>OMC Workshops data</td><td>Primary / personal data</td></tr>
<tr><td>8</td><td>OMC Webinar data</td><td>Primary / personal data</td></tr>
<tr><td>9</td><td>Matchmaking platform</td><td>Primary data</td></tr>
<tr><td>10</td><td>PCP Challenge brief</td><td>Primary data</td></tr>
</table>
</td>
</tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td>11</td><td>Call for tender applicants' data</td><td>Primary data</td></tr>
<tr><td>12</td><td>Call for tender documentation (Prior Information notice; tender specifications, tender criteria, etc.)</td><td>Primary / personal data</td></tr>
<tr><td>13</td><td>Framework Agreement</td><td>Primary / personal data</td></tr>
<tr><td>14</td><td>Specific Phase contracts</td><td>Primary / personal data</td></tr>
<tr><td>15</td><td>User's Prototype data</td><td>Primary / personal data /</td></tr>
<tr><td>16</td><td>Stakeholder's Prototype data</td><td></td></tr>
<tr><td>17</td><td>Field-testing data</td><td>Personal data/ sensitive and ultra-sensitive data</td></tr>
<tr><td>18</td><td>Impact assessment evaluation</td><td>Primary data</td></tr>
</table>
</td></tr>
<tr><td>What types of data do you expect to be processed / generated? Please refer to both special categories of personal data and non-special categories.</td><td>As described in the previous table, the data is Primary / Personal Data. Only during the field testing could there be the processing of sensitive data.</td></tr>
<tr><td>Please explain the relation of the data processing/generation (for each data type) to the objectives of the project.</td><td>
<table>
<tr><th>n.</th><th>DATA SETS</th><th>iProcureSecurity PCP Objectives</th></tr>
<tr><td>1</td><td>Stakeholders contact collection</td><td>Focus Group and OMC</td></tr>
<tr><td>2</td><td>State-of-the-art overview collection</td><td>Requirements for Triage Management Systems for Emergency Medical Services</td></tr>
<tr><td>3</td><td>Market solutions overview</td><td>OMC</td></tr>
<tr><td>4</td><td>Demand-side and supply-side questionnaires</td><td>OMC</td></tr>
<tr><td>5</td><td>Expert interview data</td><td>Focus Group and OMC</td></tr>
<tr><td>6</td><td>Focus groups data</td><td>Focus Group and OMC</td></tr>
<tr><td>7</td><td>OMC Workshops data</td><td>OMC</td></tr>
<tr><td>8</td><td>OMC Webinar data</td><td>OMC</td></tr>
<tr><td>9</td><td>Matchmaking platform</td><td>OMC</td></tr>
</table>
</td></tr>
</table>

	10	PCP Challenge brief	Call for Tender
	11	Call for tender applicants' data	Call for Tender
	12	Call for tender documentation (Prior Information notice; tender specifications, tender criteria, etc.)	Call for Tender
	13	Framework Agreement	Call for Tender
	14	Specific Phase contracts	Call for Tender
	15	User's Prototype data	Prototype Phase
	16	Stakeholder's Prototype data	Prototype Phase
	17	Field-testing data	Field-testing Phase
	18	Impact assessment evaluation	-
How will you be processing the data? Provide separate answers for each data type/category you will be processing, collecting, or generating.	**n.**	**DATA SETS**	**ORIGIN**
	1	Stakeholders contact collection	only the operators authorized by the ASLBN, who will be part of the iProcureSecurity PCP team, will be able to collect, process and archive the data in compliance with the organizational and technical measures provided by the coordinator and the ASLBN.
	2	State-of-the-art overview collection	
	3	Market solutions overview	
	4	Demand-side and supply-side questionnaires	
	5	Expert interview data	
	6	Focus groups data	
	7	OMC Workshops data	
	8	OMC Webinar data	
	9	Matchmaking platform	
	10	PCP Challenge brief	
	11	Call for tender applicants' data	
	12	Call for tender documentation (Prior Information notice; tender specifications, tender criteria, etc.)	
	13	Framework Agreement	
	14	Specific Phase contracts	

	15	User's Prototype data	
	16	Stakeholder's Prototype data	
	17	Field-testing data	
	18	Impact assessment evaluation	

For each data type, please state the format(s) in which you expect that type of data to be collected/generated. For example, numerical data, image data, text sequences, audio data etc.

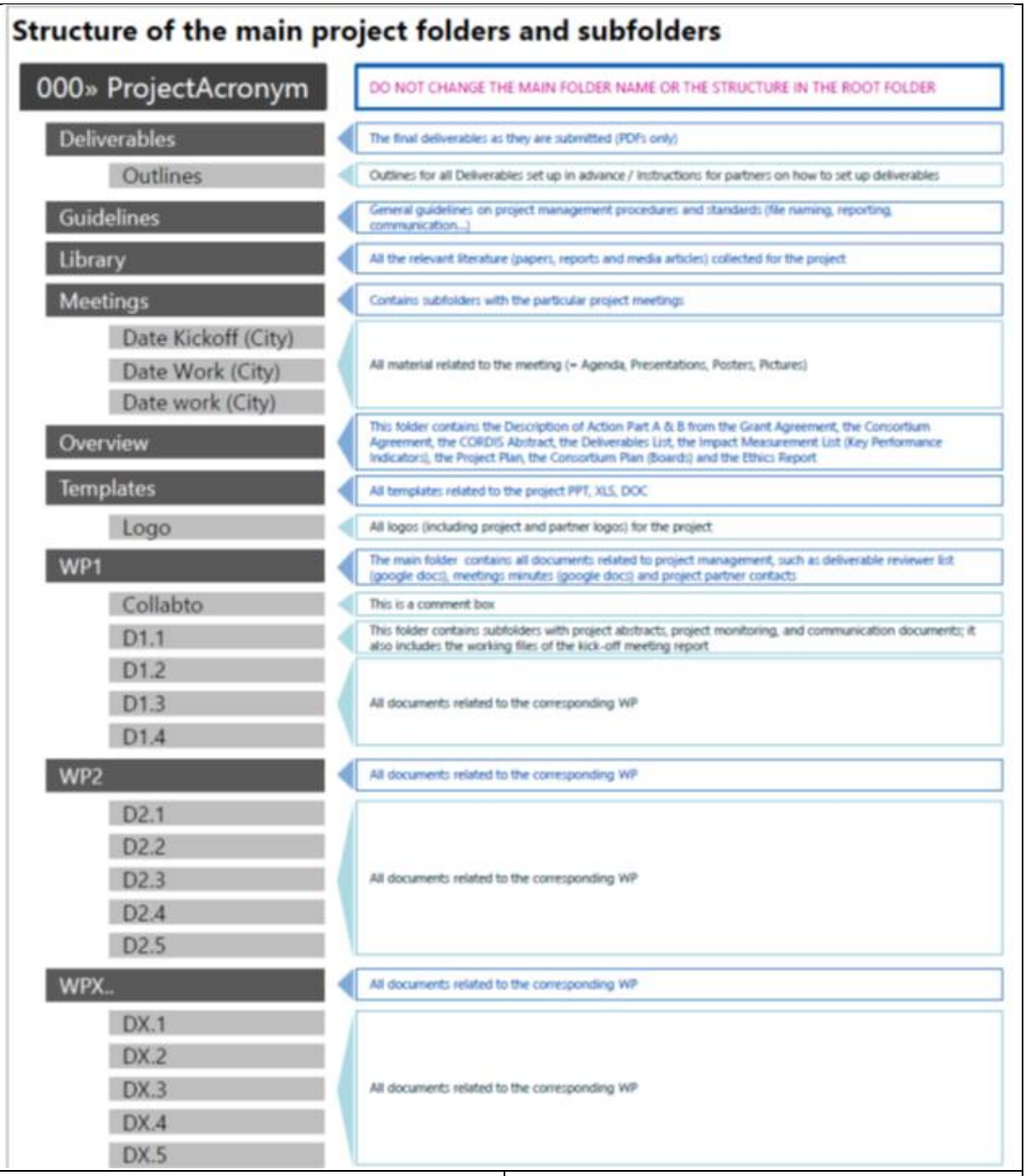
n.	DATA SETS	Data type
1	Stakeholders contact collection	.xlsx report
2	State-of-the-art overview collection	.docx – .xlsx - .pdf report
3	Market solutions overview	.docx, .xlsx, .jpeg, .pdf, Report – Document – image - video
4	Demand-side and supply-side questionnaires	.docx, .xlsx, Report
5	Expert interview data	.docx, .xlsx, Report
6	Focus groups data	.docx, .xlsx, .jpeg, Report – Document – image -video
7	OMC Workshops data	.docx, .xlsx, .jpeg, Report – Document – image -video
8	OMC Webinar data	.docx, .xlsx, .jpeg, .mpeg, Report – Document – image - video
9	Matchmaking platform	Text-neric data on platform - .xlsx report
10	PCP Challenge brief	.docx – .xlsx report
11	Call for tender applicants' data	.docx – .xlsx - .pdf report
12	Call for tender documentation (Prior Information notice; tender specifications, tender criteria, etc.)	.docx – .xlsx - .pdf report/document - .xlm for EU eNotice Platform
13	Framework Agreement	.docx – .pdf document
14	Specific Phase contracts	.docx – .pdf document
15	User's Prototype data	.docx, .xlsx, .jpeg, .pdf, Report – Document – image - video

	16	Stakeholder's Prototype data	.docx, .xlsx, .jpeg, .pdf, Report – Document – image - video
	17	Field-testing data	.docx, .xlsx, .jpeg, .pdf, Report – Document – image - video – XLM – HL7 – dicom Health report
	18	Impact assessment evaluation	.docx, .xlsx, .jpeg, .pdf, Report – Document
For each type of data what is the expected size?	Between 10 Kb to 100 MB		

Data Management Procedures	
Does your organization have data management guidelines? If so, what are they?	For data management, compliance with GDPR requirements, ASL Benevento has adopted the ASLBN Data Protection Management System with approval of the relative manual. This document can be downloaded from the company website www.aslbeneveto1.it in the privacy section
Does your organization have a data protection or security policy that you will follow? If so, what is it?	General Manager Resolution no. 391 of 05/08/2019 - EU Regulation 679/2016 relating to the protection of personal data (GDPR). Adoption of the Data Protection Management System and approval of the relative manual. Below is a link to all the actions taken for data protection and security http://www.aslbenevento1.it/modules.php?name=Sections&op=viewarticle&artid=297
Does your organization have a Research Data Management policy? What is it?	No
Are there any formal standards you will adopt when processing data for the project?	The personal data are processed with IT tools or paper means, furthermore other methods deemed useful may be used on a case-by-case basis, by telephone and by mail or verbally, always in compliance with the principles of the EU Regulation and the ASLBN' Procedures and Guidelines. The Consortium Partners keep the personal data for the time necessary to fulfil legal obligations and the data is stored in paper or computer

	archives protected with the appropriate security measures provided by current legislation, able to guarantee that only authorized operators can know the information concerning personal data. The Consortium Partners also adopt adequate technical-organizational security measures pursuant to art. 30 of the EU Regulation
Please provide the contact details of your organization's DPO.	Data Protection Officer Alberto Lombardi ASL BENEVENTO Pec. dpo@pec.aslbenevento.it

Documentation, Organization and Storage	
Who will be responsible for documentation, organization, and storage?	The person responsible for documentation, organization, and storage is the Director of ASLBN Procurement Department, and the workers of ASLBN IP-Office.
How will you label and organize data, records, and files?	



How long will you be storing personal data generated in the project for?	The data collected will be stored for a 5-year period in order to comply with the European Union requirements for possible audits of the results of the project. The data will be deleted as soon as they are no longer necessary for their purpose, adopting the security measures to ensure the pseudonymization or total destruction of them.
How and where will the data be stored?	The Data are stored in the google drive Consortium folder (https://drive.google.com/drive/folders/1b2ubEIndlOB6Dp5FGmr3UUiPgsrYyJ_G?usp=sharing)

	+ a local folder on a PC located in the perimeter network of the Benevento ASL, which has the same structure as the folder shared with the consortium, but which also contains working draft documents and confidential documents
Are you using proprietary file formats to generate and store your research data? If so, will the documentation about the software needed to access the data be included?	No
If data are collected with mobile devices, how will you transfer and store the data?	The data aren't collected with mobile devices.
If data are held in various places, how will you keep track of versions?	We have a table of content of Documents (.doc.,.xls,.,pdf,.jpeg…) that indicate the version and the stored data

Access	
Who within your organization will manage access to this data?	The Personal Data Controllers, for the purposes of the General Data Protection Regulation (GDPR), are the ASLBN General Director. The ASLBN internal processors are the departments' managers that provide the specific services of the project. All the other operators that process personal data, even for integrated projects, are to be considered "persons authorized to process" and as such adequately trained in the regulatory principles regarding the personal data protection.
Who within your organization will have access to the data processed for the iProcureSecurity PCP project?	The ASLBN internal Processor of iProcureSecurity PCP Personal Data is the Procurement department manager that provide the specific services of the project. All the members of ASLBN team, that process iProcureSecurity PCP data, even for integrated projects, are to be considered "persons authorized to process" and as such adequately trained in the regulatory principles regarding the personal data protection.
How will the identity of the person accessing the data be ascertained?	The ASLBN Team operators who access the data and project documents on the shared company folder must authenticate with user and password.

Will there by conditions to gaining data access? If so, what will those conditions be?	Only the members of ASLBN team will process iProcureSecurity PCP data The personal data are not subject to disclosure (i.e. they cannot be disclosed to an indistinct number of subjects). The analysis of the results will be anonymous, that is no one will know who the data belongs to. The information will be processed during the analysis of the data obtained and will appear in the project deliverables - but again, only in a way that will not allow anybody to identify from whom we received the information.
What methods or software tools will be needed to access the data? Will any other accompanying information be required to properly interpret the data?	use of access and authorization credentials
What information, if any needs to be retained in order for the data to be read and interpreted in the future?	Name (data), type (data), latest version, data of the latest version, operator who makes the last modification, since the last modification, operator who created the document (data), document creation date (data).
Will any data be made openly available for all project partners?	The iProcureSecurity PCP project could deposit the data generated and collected that will be made openly available in an open online research data repository. Now ALSBN don't use pen online research data repository but it's possible use of a specific platform as the ZENODO platform (for example).
How will the data that is made openly available be maintained? In a repository?	In data repository

Sharing	
What data will be shared?	In the PHASE 0 -PHASE 1 – PHASE 2 - PHASE Types of personal data that we collect and process: - Personal Identification Data. - Surveys and personal interviews - Notes, audio and/or video recordings of your activities that may be made during Co-creative workshops and multidisciplinary focus groups. - Additional information that you provide may be used in the dissemination and

	promotion of iProcureSecurity PCP in general. - Filed Testing Data No other use will be made of them without your written permission
When will data be shared?	During the different projects' phase
For what purposes of the project will data be shared?	The data sharing by the iProcureSecurity PCP Consortium is necessary when managing award procedures (OMC, procurement, experts) and managing the execution of contracts (procurement, experts) and the implementation of agreements concluded during the procedures. These processing operations are under the responsibility of the Partners as Controllers, regarding the collection and processing of personal data. In particular the Consortium will hold an Open Market Consultation (OMC) with potential tenderers and end-users to broach the views of the market about our scope. The purpose of the OMC is to canvass wide stakeholder opinion on the suitability of iProcureSecurity PCP. With the market consultation, the consortium will get an insight into the market, the state of the art and future developments in order to prepare an adequate procurement with the right and feasible scope. The answers to any of the iProcureSecurity PCP OMC questionnaires will be used for research purposes only under the frame of the iProcureSecurity PCP project. Personal data will not be used for any automated decision-making including profiling.
Who will data be shared with?	The data will be shared among the Partners staff participating in the project. So the partners' internal processors are the departments' managers that provide the specific services of the project. All the other operators that process personal data, even for integrated projects, are to be considered "*persons authorized to process*" and as such adequately trained in the regulatory principles regarding the personal data protection.

Does sharing raise any privacy, ethical, or confidentiality concerns? If yes, what are they and why?	The sharing of data has no problems inherent to the GDPR as long as the compliance measures with the GDPR and all the operators that process personal data, are appointed as "*persons authorized to process*"
Will a data sharing agreement be required? If some data categories and types are kept closed provide a rationale for doing so.	no

Security	
What are the major risks to data security?	the major data security risks: • destruction or loss, even accidental, of data, • unauthorized access; • processing that is not permitted or does not comply with the purposes of the collection, • modification of data as a result of unauthorized or non-compliant interventions. • Viruses, Data phishing, Cyber attack
How will each of these risks be managed?	Security measures, adopted by Consortium, are a set of technological, procedural and organizational requirements aimed at implementing an adequate level of security in data processing, in order to guarantee the confidentiality, integrity and availability of data and the resilience of the systems. The Technical measures aimed at guaranteeing the confidentiality, integrity and availability of data and the resilience of the systems are described below: 1. Security tools for paper documents and archives 2. Security tools applied to data Security tools applied to systems (Spyware virus protection measures, Perimeter logical security measures, Backup and replacement of data storage, etc..)
Do you need to anonymize any of the data?	No
What security measures do you anticipate being required for safe data storage, sharing and management?	- Security tools applied to data: a. Management of assignment and management of access privileges (profiling) and credentials with enabling and disabling of accounts; b. Logical access control and traceability systems; c. Application log management; d. Encryption of data in company DBs;

	- Security tools applied to systems: a. Perimeter logical security measures through firewalls and DMZs; b. Spyware virus protection measures etc .; c. Use of secure network protocols for accessing applications; d. Use of network protocols and secure applications for data transmission; e. Backup and replacement of data storage; f. Systems updating and patching (with respect to the application);
Have you implemented or outlined any procedures to follow in the case of a data breach? If so, what are they?	In compliance with the provisions of art. 33 of EU Regulation 2016/679, the ASL Benevento has drawn up a procedure in order to guarantee, according to a standardized process, the actions to be implemented in the event of concrete, potential or suspected violations of personal data and to be able to find the Guarantor Authority and / or interested parties within the times and in the manner provided for by European legislation and without undue delay.
Are your digital and non-digital data, and any copies, held in a safe and secure location?	ASLBN uses secure systems for filing paper documents (cabinets, filing cabinets, etc., equipped with locks).

Ethical Considerations	
What types of special category personal data do you intend to generate/process?	In the PHASE 0 -PHASE 1 – PHASE 2 Types of personal data that we collect and process: - Personal Identification Data. - Surveys and personal interviews - Notes, audio and/or video recordings of your activities that may be made during Co-creative workshops and multidisciplinary focus groups. - Additional information that you provide may be used in the dissemination and promotion of iProcureSecurity PCP in general. No other use will be made of them without your written permission In the PHASE 3

	- possibility of using health and sensitive data for the cluster of users participating in the field test
- Will any of the data subjects be children?	No
Will any of the data subjects be vulnerable people?	No
Will you be collecting personal or sensitive data from people who have not given their explicit consent to participate in the Project?	No
For each category of data you intend to collect, please provide: • If the data is personal data, as defined by the GDPR, which of the six Art. 6 bases will you rely on for the processing of each category of personal data? If the data is sensitive data, as defined by the GDPR, which of the ten Art. 9 bases will you rely on for the processing of each category of sensitive data?	• Art. 6 par. 1(a) consent (from webinar and interviews participants and for partners' images and voice) • Art. 6 par. 1(b) contract (for partners' names and contact details) • Art. 9 par. 2 (a) consent (for webinar participants' data, for field testing participant data).
Have you already gained consent for data preservation and sharing from any data subject(s)?	Yes, for the following activities: - registration for events related to the project - Participation in Focus Groups and project Committee
Will you engage in large scale or big data processing?	No
Will any entity (including any service provider) outside of the E.U. have access to personal or sensitive data? If so, who? For what purpose? Where is each of these entities located?	Some non-sensitive data may be provided to Project Partners based in Turkey (AAHD, IBB) for the sole purpose of carrying out project activities.

AGENZIA REGIONALE EMERGENZA URGENZA, AREU

Table 8: **AREU DMP Questionnaire**

Data Description	
What type of data will you collect? Please provide in brief.	In the PHASE 0 -PHASE 1 – PHASE 2 Types of personal data that we collect and process:

<table>
<tr>
<td></td>
<td>
- Personal Identification Data.
- Surveys and personal interviews
- Notes, audio and/or video recordings of your activities that may be made during Co-creative workshops and multidisciplinary focus groups.
- Additional information that you provide may be used in the dissemination and promotion of iProcureSecurity PCP in general.

No other use will be made of them without your written permission
In the PHASE 3
- possibility of using health and sensitive data for the cluster of users participating in the field test
-
<table>
<tr><th>n.</th><th>DATA SETS</th></tr>
<tr><td>1</td><td>Stakeholders contact collection</td></tr>
<tr><td>2</td><td>State-of-the-art overview collection</td></tr>
<tr><td>3</td><td>Market solutions overview</td></tr>
<tr><td>4</td><td>Demand-side and supply-side questionnaires</td></tr>
<tr><td>5</td><td>Expert interview data</td></tr>
<tr><td>6</td><td>Focus groups data</td></tr>
<tr><td>7</td><td>OMC Workshops data</td></tr>
<tr><td>8</td><td>OMC Webinar data</td></tr>
<tr><td>9</td><td>Matchmaking platform</td></tr>
<tr><td>10</td><td>PCP Challenge brief</td></tr>
<tr><td>11</td><td>Call for tender applicants’ data</td></tr>
<tr><td>12</td><td>Call for tender documentation (Prior Information notice; tender specifications, tender criteria, etc.)</td></tr>
<tr><td>13</td><td>Framework Agreement</td></tr>
<tr><td>14</td><td>Specific Phase contracts</td></tr>
<tr><td>15</td><td>User’s Prototype data</td></tr>
<tr><td>16</td><td>Stakeholder’s Prototype data</td></tr>
<tr><td>17</td><td>Field-testing data</td></tr>
<tr><td>18</td><td>Impact assessment evaluation</td></tr>
</table>
</td>
</tr>
<tr>
<td>What is the purpose of the data collection?</td>
<td>The iProcureSecurity PCP Consortium is committed to protect personal data and to respect data subject’s privacy. Our Partners' lawful bases for processing personal data, as set out in Article 6 of the GDPR, vary depending on the particular processed personal data whose they refer with.</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>The participation in the study is completely voluntary.

The data collection is related to

- Co-creative workshops to stimulate new ideas.
- Surveys and personal interviews to assess the needs and possible innovations.
- Multidisciplinary focus groups for needs analysis.

The main purpose of the evaluation is to gather information about expert opinion regarding the shortcomings of the medical emergency system, the possibilities of improvement through innovation and to gather the requirements for the prototypes.

The information collected in the study will be anonymised and the personal data stored in an encrypted way.

Personal data will not be used for any automated decision-making including profiling.</td>
</tr>
<tr>
<td>Please explain:
• What is the origin of the data?
• Are you using data someone else produced? If so, where is it from?</td>
<td>
<table>
<tr><th>n.</th><th>DATA SETS</th><th>ORIGIN</th></tr>
<tr><td>1</td><td>Stakeholders contact collection</td><td>Publicly available data</td></tr>
<tr><td>2</td><td>State-of-the-art overview collection</td><td>Publicly available data</td></tr>
<tr><td>3</td><td>Market solutions overview</td><td>Publicly available data</td></tr>
<tr><td>4</td><td>Demand-side and supply-side questionnaires</td><td>Primary data</td></tr>
<tr><td>5</td><td>Expert interview data</td><td>Primary / personal data</td></tr>
<tr><td>6</td><td>Focus groups data</td><td>Primary data</td></tr>
<tr><td>7</td><td>OMC Workshops data</td><td>Primary / personal data</td></tr>
<tr><td>8</td><td>OMC Webinar data</td><td>Primary / personal data</td></tr>
<tr><td>9</td><td>Matchmaking platform</td><td>Primary data</td></tr>
<tr><td>10</td><td>PCP Challenge brief</td><td>Primary data</td></tr>
<tr><td>11</td><td>Call for tender applicants’ data</td><td>Primary data</td></tr>
</table>
</td>
</tr>
</table>

<table>
<tr><td></td><td>12</td><td>Call for tender documentation (Prior Information notice; tender specifications, tender criteria, etc.)</td><td>Primary / personal data</td></tr>
<tr><td></td><td>13</td><td>Framework Agreement</td><td>Primary / personal data</td></tr>
<tr><td></td><td>14</td><td>Specific Phase contracts</td><td>Primary / personal data</td></tr>
<tr><td></td><td>15</td><td>User’s Prototype data</td><td>Primary / personal data /</td></tr>
<tr><td></td><td>16</td><td>Stakeholder’s Prototype data</td><td></td></tr>
<tr><td></td><td>17</td><td>Field-testing data</td><td>Personal data/ sensitive and ultra-sensitive data</td></tr>
<tr><td></td><td>18</td><td>Impact assessment evaluation</td><td>Primary data</td></tr>
<tr><td>What types of data do you expect to be processed / generated? Please refer to both special categories of personal data and non-special categories.</td><td colspan="3">As described in the previous table, the data is Primary / Personal Data. Only during the field testing could there be the processing of sensitive data.</td></tr>
<tr><td>Please explain the relation of the data processing/generation (for each data type) to the objectives of the project.</td><td>n.</td><td>DATA SETS</td><td>iProcureSecurity PCP Objectives</td></tr>
<tr><td></td><td>1</td><td>Stakeholders contact collection</td><td>Focus Group and OMC</td></tr>
<tr><td></td><td>2</td><td>State-of-the-art overview collection</td><td>Requirements for Triage Management Systems for Emergency Medical Services</td></tr>
<tr><td></td><td>3</td><td>Market solutions overview</td><td>OMC</td></tr>
<tr><td></td><td>4</td><td>Demand-side and supply-side questionnaires</td><td>OMC</td></tr>
<tr><td></td><td>5</td><td>Expert interview data</td><td>Focus Group and OMC</td></tr>
<tr><td></td><td>6</td><td>Focus groups data</td><td>Focus Group and OMC</td></tr>
<tr><td></td><td>7</td><td>OMC Workshops data</td><td>OMC</td></tr>
</table>

	8	OMC Webinar data	OMC
	9	Matchmaking platform	OMC
	10	PCP Challenge brief	Call for Tender
	11	Call for tender applicants' data	Call for Tender
	12	Call for tender documentation (Prior Information notice; tender specifications, tender criteria, etc.)	Call for Tender
	13	Framework Agreement	Call for Tender
	14	Specific Phase contracts	Call for Tender
	15	User's Prototype data	Prototype Phase
	16	Stakeholder's Prototype data	Prototype Phase
	17	Field-testing data	Field-testing Phase
	18	Impact assessment evaluation	-

How will you be processing the data? Provide separate answers for each data type/category you will be processing, collecting, or generating.	**n.**	**DATA SETS**	**ORIGIN**
	1	Stakeholders contact collection	only the operators authorized by AREU, who will be part of the iProcureSecurity PCP team, will be able to collect, process and archive the data in compliance
	2	State-of-the-art overview collection	
	3	Market solutions overview	
	4	Demand-side and supply-side questionnaires	
	5	Expert interview data	
	6	Focus groups data	
	7	OMC Workshops data	

	8	OMC Webinar data	with the organizational and technical measures provided by the coordinator and the AREU.
	9	Matchmaking platform	
	10	PCP Challenge brief	
	11	Call for tender applicants' data	
	12	Call for tender documentation (Prior Information notice; tender specifications, tender criteria, etc.)	
	13	Framework Agreement	
	14	Specific Phase contracts	
	15	User's Prototype data	
	16	Stakeholder's Prototype data	
	17	Field-testing data	
	18	Impact assessment evaluation	

For each data type, please state the format(s) in which you expect that type of data to be collected/generated. For example, numerical data, image data, text sequences, audio data etc.	**n.**	**DATA SETS**	**Data type**
	1	Stakeholders contact collection	.xlsx report
	2	State-of-the-art overview collection	.docx – .xlsx - .pdf report
	3	Market solutions overview	.docx, .xlsx, .jpeg, .pdf, Report – Document – image -video
	4	Demand-side and supply-side questionnaires	.docx, .xlsx, Report
	5	Expert interview data	.docx, .xlsx, Report
	6	Focus groups data	.docx, .xlsx, .jpeg, Report – Document – image -video

	7	OMC Workshops data	.docx, .xlsx, .jpeg, Report – Document – image -video
	8	OMC Webinar data	.docx, .xlsx, .jpeg, .mpeg, Report – Document – image -video
	9	Matchmaking platform	Text-neric data on platform - .xlsx report
	10	PCP Challenge brief	.docx – .xlsx report
	11	Call for tender applicants' data	.docx – .xlsx - .pdf report
	12	Call for tender documentation (Prior Information notice; tender specifications, tender criteria, etc.)	.docx – .xlsx - .pdf report/document - .xlm for EU eNotice Platform
	13	Framework Agreement	.docx – .pdf document
	14	Specific Phase contracts	.docx – .pdf document
	15	User's Prototype data	.docx, .xlsx, .jpeg, .pdf, Report – Document – image -video
	16	Stakeholder's Prototype data	.docx, .xlsx, .jpeg, .pdf, Report – Document – image -video
	17	Field-testing data	.docx, .xlsx, .jpeg, .pdf, Report – Document – image -video –

			XLM – HL7 – dicom Health report
	18	Impact assessment evaluation	.docx, .xlsx, .jpeg, .pdf, Report – Document
For each type of data what is the expected size?	Between 10 Kb to 100 MB		

Data Management Procedures	
Does your organization have data management guidelines? If so, what are they?	For data management, compliance with GDPR requirements, AREU has adopted the "*REGOLAMENTO 32 REGOLAMENTO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI in applicazione del Codice in materia di protezione dei dati personali ex D.Lgs. n. 196 del 30 giugno 2003 e s.m.i.*". This document, approved by the General Director is available on equest.
Does your organization have a data protection or security policy that you will follow? If so, what is it?	See the point above.
Does your organization have a Research Data Management policy? What is it?	No
Are there any formal standards you will adopt when processing data for the project?	The personal data are processed with IT tools or paper means, furthermore other methods deemed useful may be used on a case-by-case basis, by telephone and by mail or verbally, always in compliance with the principles of the EU Regulation and the AREU Procedures and Guidelines. The Consortium Partners keep the personal data for the time necessary to fulfil legal obligations and the data is stored in paper or computer archives protected with the appropriate security measures provided by current legislation, able to guarantee that only authorized operators can know the information concerning personal data. The Consortium Partners also adopt adequate technical-organizational security measures pursuant to art. 30 of the EU Regulation
Please provide the contact details of your organization's DPO.	AREU DPO

	Avv. Alessandro Ovadia "Resp. Protezione Dati" dpo@areu.lombardia.it

Documentation, Organization and Storage	
Who will be responsible for documentation, organization, and storage?	The person responsible for documentation, organization, and storage is the AREU General Director together with the responsibles of the agency departments, as stated in the above "Regolamento".
How will you label and organize data, records, and files?	To be determined at a later stage

Structure of the main project folders and subfolders

How long will you be storing personal data generated in the project for?	The data collected will be stored for a 5-year period in order to comply with the European Union requirements for possible audits of the results of the project. The data will be deleted as soon as they are no longer necessary for their purpose, adopting the security measures to ensure the pseudonymization or total destruction of them.
How and where will the data be stored?	The Data are stored in the google drive Consortium folder (https://drive.google.com/drive/folders/1b2ubEIndlOB6Dp5FGmr3UUiPgsrYyJ_G?usp=sharing) and in the intranet of AREU.
Are you using proprietary file formats to generate and store your research data? If so, will the documentation about the software needed to access the data be included?	No
If data are collected with mobile devices, how will you transfer and store the data?	The data aren't collected with mobile devices.
If data are held in various places, how will you keep track of versions?	We have a table of content of Documents (.doc.,.xls,.,pdf,.jpeg…) that indicate the version and the stored data

Access	
Who within your organization will manage access to this data?	The Personal Data Controllers, for the purposes of the General Data Protection Regulation (GDPR), is the AREU General Director. The AREU internal processors are the departments' managers that provide the specific services of the project. All the other operators that process personal data, even for integrated projects, are to be considered "persons authorized to process" and as such adequately trained in the regulatory principles regarding the personal data protection.
Who within your organization will have access to the data processed for the iProcureSecurity PCP project?	The AREU internal Processor of iProcureSecurity PCP Personal Data is the Procurement department manager that provide the specific services of the project. All the members of AREU team, that process iProcureSecurity PCP data, even for integrated projects, are to be considered "persons authorized to process" and as such adequately

	trained in the regulatory principles regarding the personal data protection.
How will the identity of the person accessing the data be ascertained?	The AREU Team operators who access the data and project documents on the shared company folder must authenticate with user and password.
Will there by conditions to gaining data access? If so, what will those conditions be?	Only the members of AREU team will process iProcureSecurity PCP data The personal data are not subject to disclosure (i.e. they cannot be disclosed to an indistinct number of subjects). The analysis of the results will be anonymous, that is no one will know who the data belongs to. The information will be processed during the analysis of the data obtained and will appear in the project deliverables - but again, only in a way that will not allow anybody to identify from whom we received the information.
What methods or software tools will be needed to access the data? Will any other accompanying information be required to properly interpret the data?	use of access and authorization credentials
What information, if any needs to be retained in order for the data to be read and interpreted in the future?	Name (data), type (data), latest version, data of the latest version, operator who makes the last modification, since the last modification, operator who created the document (data), document creation date (data).
Will any data be made openly available for all project partners?	The iProcureSecurity PCP project could deposit the data generated and collected that will be made openly available in an open online research data repository.
How will the data that is made openly available be maintained? In a repository?	In data repository

Sharing	
What data will be shared?	In the PHASE 0 -PHASE 1 – PHASE 2 - PHASE Types of personal data that we collect and process: - Personal Identification Data. - Surveys and personal interviews - Notes, audio and/or video recordings of your activities that may be made during

	Co-creative workshops and multidisciplinary focus groups. - Additional information that you provide may be used in the dissemination and promotion of iProcureSecurity PCP in general. - Filed Testing Data No other use will be made of them without your written permission
When will data be shared?	During the different projects' phase
For what purposes of the project will data be shared?	The data sharing by the iProcureSecurity PCP Consortium is necessary when managing award procedures (OMC, procurement, experts) and managing the execution of contracts (procurement, experts) and the implementation of agreements concluded during the procedures. These processing operations are under the responsibility of the Partners as Controllers, regarding the collection and processing of personal data. In particular the Consortium will hold an Open Market Consultation (OMC) with potential tenderers and end-users to broach the views of the market about our scope. The purpose of the OMC is to canvass wide stakeholder opinion on the suitability of iProcureSecurity PCP. With the market consultation, the consortium will get an insight into the market, the state of the art and future developments in order to prepare an adequate procurement with the right and feasible scope. The answers to any of the iProcureSecurity PCP OMC questionnaires will be used for research purposes only under the frame of the iProcureSecurity PCP project. Personal data will not be used for any automated decision-making including profiling.
Who will data be shared with?	The data will be shared among the Partners staff participating in the project. So the partners' internal processors are the departments' managers that provide the specific services of the project. All the other operators that process personal data, even for integrated projects, are to be considered "*persons authorized to process*" and

	as such adequately trained in the regulatory principles regarding the personal data protection.
Does sharing raise any privacy, ethical, or confidentiality concerns? If yes, what are they and why?	The sharing of data has no problems inherent to the GDPR as long as the compliance measures with the GDPR and all the operators that process personal data, are appointed as "*persons authorized to process*"
Will a data sharing agreement be required? If some data categories and types are kept closed provide a rationale for doing so.	no

Security	
What are the major risks to data security?	the major data security risks: • destruction or loss, even accidental, of data, • unauthorized access; • processing that is not permitted or does not comply with the purposes of the collection, • modification of data as a result of unauthorized or non-compliant interventions. • Viruses, Data phishing, Cyber attack
How will each of these risks be managed?	Security measures, adopted by Consortium, are a set of technological, procedural and organizational requirements aimed at implementing an adequate level of security in data processing, in order to guarantee the confidentiality, integrity and availability of data and the resilience of the systems. The Technical measures aimed at guaranteeing the confidentiality, integrity and availability of data and the resilience of the systems are described below: 3. Security tools for paper documents and archives 4. Security tools applied to data Security tools applied to systems (Spyware virus protection measures, Perimeter logical security measures, Backup and replacement of data storage, etc..)
Do you need to anonymize any of the data?	No
What security measures do you anticipate being required for safe data storage, sharing and management?	- Security tools applied to data: a. Management of assignment and management of access privileges (profiling) and credentials with enabling and disabling of accounts;

	b. Logical access control and traceability systems; c. Application log management; d. Encryption of data in company DBs; - Security tools applied to systems: a. Perimeter logical security measures through firewalls and DMZs; b. Spyware virus protection measures etc .; c. Use of secure network protocols for accessing applications; d. Use of network protocols and secure applications for data transmission; e. Backup and replacement of data storage; f. Systems updating and patching (with respect to the application);
Have you implemented or outlined any procedures to follow in the case of a data breach? If so, what are they?	In compliance with the provisions of art. 33 of EU Regulation 2016/679, the AREU has drawn up a procedure in order to guarantee, according to a standardized process, the actions to be implemented in the event of concrete, potential or suspected violations of personal data and to be able to find the Guarantor Authority and / or interested parties within the times and in the manner provided for by European legislation and without undue delay.
Are your digital and non-digital data, and any copies, held in a safe and secure location?	AREU uses secure systems for filing paper documents (cabinets, filing cabinets, etc., equipped with locks).

Ethical Considerations	
What types of special category personal data do you intend to generate/process?	In the PHASE 0 -PHASE 1 – PHASE 2 Types of personal data that we collect and process: - Personal Identification Data. - Surveys and personal interviews - Notes, audio and/or video recordings of your activities that may be made during Co-creative workshops and multidisciplinary focus groups. - Additional information that you provide may be used in the dissemination and promotion of iProcureSecurity PCP in general.

	No other use will be made of them without your written permission In the PHASE 3 - possibility of using health and sensitive data for the cluster of users participating in the field test
- Will any of the data subjects be children?	No
Will any of the data subjects be vulnerable people?	No
Will you be collecting personal or sensitive data from people who have not given their explicit consent to participate in the Project?	No
For each category of data you intend to collect, please provide: • If the data is personal data, as defined by the GDPR, which of the six Art. 6 bases will you rely on for the processing of each category of personal data? If the data is sensitive data, as defined by the GDPR, which of the ten Art. 9 bases will you rely on for the processing of each category of sensitive data?	• Art. 6 par. 1(a) consent (from webinar and interviews participants and for partners' images and voice) • Art. 6 par. 1(b) contract (for partners' names and contact details) • Art. 9 par. 2 (a) consent (for webinar participants' data, for field testing participant data).
Have you already gained consent for data preservation and sharing from any data subject(s)?	- At the moment all the subjects providing data are AREU team members.
Will you engage in large scale or big data processing?	No
Will any entity (including any service provider) outside of the E.U. have access to personal or sensitive data? If so, who? For what purpose? Where is each of these entities located?	Some non-sensitive data may be provided to Project Partners based in Turkey (AAHD, IBB) for the sole purpose of carrying out project activities.

ELLINIKOS ERYTHROS STAVROS, HRC

Table 9: **HRC DMP Questionnaire**

Data Description	
What type of data will you collect? Please provide in brief.	HRC will provide Open Market Consultation, that's why SME, Industry and previous projects

	will be collected. This information is available in the web page (public available information). End user requirements in the means of specifications, desired features, usability and performance among others. That does not have personal questions.
What is the purpose of the data collection?	Making informed decision and ensure the quality in the provision of services
Please explain: What is the origin of the data? Are you using data someone else produced? If so, where is it from?	• Focus groups and interviews with practitioners and experts. • OMCs data • Piloting and testing generated data All data is collected inside the organization; thus, no external data is used.
What types of data do you expect to be processed / generated? Please refer to both special categories of personal data and non-special categories.	Numerical, personal (text and numbers), image data
Please explain the relation of the data processing/generation (for each data type) to the objectives of the project.	All data processed by HRC in the framework of the project will facilitate the triage process.
How will you be processing the data? Provide separate answers for each data type/category you will be processing, collecting, or generating.	Real time processing for both types of data.
For each data type, please state the format(s) in which you expect that type of data to be collected/generated. For example, numerical data, image data, text sequences, audio data etc.	Checklists for numerical data, Interviews, Surveys or Questionnaires for personal data
For each type of data what is the expected size?	Manageable size (bytes-kilobytes) except for image data, which is expected to be of gigabyte size

Data Management Procedures	
Does your organization have data management guidelines? If so, what are they?	Yes. Data management guidelines are related to the collection, access, analysis and storage procedures which best serve to comply with GDPR guidelines for protection of personal data processed at the Hellenic Red Cross. HRC collects and processes the Personal Data of individuals affected by Humanitarian Emergencies in order to perform humanitarian activities.

	Consent for the processing of data is central to the GDPR's guidelines. The beneficiaries are informed of why each piece of personal data is necessary for the provision of services and how this data will be processed. Also, they must be informed of their rights regarding the data collected.
Does your organization have a data protection or security policy that you will follow? If so, what is it?	Data Protection Guidelines have been developed by the HRC DPO and concern: Technical Security Measures: 1.Password Protection 2. Encryption 3. Antivirus 4. Systems Backup 5. Cloud Computing Service 6. Automatic Logout 7. Data Access Control Operational Procedures for every service (software, hardware)
Does your organization have a Research Data Management policy? What is it?	HRC has developed a data management plan which is adjusted at every research proposal if any research data are to be collected or used. The plan covers data types and volume, capture, storage, integrity, confidentiality, retention and destruction, sharing and deposit.
Are there any formal standards you will adopt when processing data for the project?	Yes, if there is a need according to the final requirements of the project
Please provide the contact details of your organization's DPO.	ADVANCED QUALITY Ltd (AQS) dpo@aqs.gr 00302106216997 Contact Person: Themistoklis Sioros

Documentation, Organization and Storage	
Who will be responsible for documentation, organization, and storage?	HRC Informatics Service
How will you label and organize data, records, and files?	Using HRC guidelines that are in compliance with GDPR. The key is that data subjects receive a unique code according to which data will be labeled and organized Unique code and name will be organized separately from other data.
How long will you be storing personal data generated in the project for?	5 years

How and where will the data be stored?	The hardcopies will be stored in a safe, locked location at the HRC HQs. The electronic archive of data will be stored at HRC server. A code (regularly updated) will be required for accessing them. Access will be allowed to data processor that will be appointed by HRC Governance.
Are you using proprietary file formats to generate and store your research data? If so, will the documentation about the software needed to access the data be included?	No. Microsoft Office 365 tool
If data are collected with mobile devices, how will you transfer and store the data?	Using KOBO toolbox. It is an open-source suite of tools for data collection and analysis in humanitarian emergencies that is used by HRC. Encryption will be used as a method for transferring data in different networks if needed. Storage will be held according to HRC guidelines described above.
If data are held in various places, how will you keep track of versions?	By numbering and dating the relevant versions.

Access	
Who within your organization will manage access to this data?	HRC Informatics Service
Who within your organization will have access to the data processed for the iProcureSecurity PCP project?	Director General of HRC
How will the identity of the person accessing the data be ascertained?	By using login and specific account
Will there by conditions to gaining data access? If so, what will those conditions be?	No, there is a securing entry to accessing data due to the structured cabling of HRC network
What methods or software tools will be needed to access the data? Will any other accompanying information be required to properly interpret the data?	KOBO toolbox
What information, if any needs to be retained in order for the data to be read and interpreted in the future?	Information related to the reporting of the project
Will any data be made openly available for all project partners?	Only to the partners which HRC will collaborate with (i.e. EKAB)
How will the data that is made openly available be maintained? In a repository?	Yes, in a repository

Sharing	

What data will be shared?	Numerical data, personal data and sensitive personal data
When will data be shared?	Throughout the different phases of the response in case of an emergency
For what purposes of the project will data be shared?	To facilitate the interoperability of different components To make informed decisions To serve the best of interest of the data subject
Who will data be shared with?	Involved parties in the scenario that concerns HRC participation
Does sharing raise any privacy, ethical, or confidentiality concerns? If yes, what are they and why?	No
Will a data sharing agreement be required? If some data categories and types are kept closed provide a rationale for doing so.	Yes

Security	
What are the major risks to data security?	1.Accidental exposure of data 2.Phishing of data 3.Data loss in the server or/and cloud
How will each of these risks be managed?	1.Intensive relevant trainings, unique strong passwords of users 2. Strong antivirus system and encryption of data 3. Regular backing up of the data to another location
Do you need to anonymize any of the data?	Numerical data regarding first response of HRC will be anonymized Sensitive Personal data concerning availabilities will kept separately from the names. They will be shared encrypted
What security measures do you anticipate being required for safe data storage, sharing and management?	1.Password Protection (high secure passwords that change regularly) 2. Encryption 3. Antivirus 4. Systems Backup 5. Data Access Control 6.Operational Procedures (software, hardware)
Have you implemented or outlined any procedures to follow in the case of a data breach? If so, what are they?	In case of data breach, data users a) Report to the HRC DPO to assess the break B) Change passwords and C) Inform the data subject
Are your digital and non-digital data, and any copies, held in a safe and secure location?	Yes. Non digital data in cupboards that are locked

	Digital data in the HRC server and cloud. Redcross account password is required to accessing them

Ethical Considerations	
What types of special category personal data do you intend to generate/process?	Personal Data and Sensitive Personal Data such as Racial or ethnic origin of the data subject Physical, mental health or condition
Will any of the data subjects be children?	No
Will any of the data subjects be vulnerable people?	No
Will you be collecting personal or sensitive data from people who have not given their explicit consent to participate in the Project?	No
For each category of data you intend to collect, please provide: • If the data is personal data, as defined by the GDPR, which of the six Art. 6 bases will you rely on for the processing of each category of personal data? • If the data is sensitive data, as defined by the GDPR, which of the ten Art. 9 bases will you rely on for the processing of each category of sensitive data?	• the data subject has given consent to the processing of his or her personal data for one or more specific purposes • the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to Article 9, in paragraph 1 of GDPR, may not be lifted by the data subject
Have you already gained consent for data preservation and sharing from any data subject(s)?	Yes
Will you engage in large scale or big data processing?	Yes, if it is required by the programme
Will any entity (including any service provider) outside of the E.U. have access to personal or sensitive data? If so, who? For what purpose? Where is each of these entities located?	Project partners AAHD and IBB from Turkey. Purpose: project activities such as OMC, webinar events, triage management system requirements, use cases.

ETHNIKO KENTRO AMESIS VOITHEIAS, EKAB

Table 10: **EKAB DMP Questionnaire**

Data Description	
What type of data will you collect? Please provide in brief.	EKAB will provide Open Market Consultation, that's why SME, Industry and previous projects will be collected. This information is available in the web page (public available information). End user requirements in the means of

	specifications, desired features, usability and performance among others. That does not include personal data.
What is the purpose of the data collection?	Create and test a tool that will support Informed medical decision.
Please explain: • What is the origin of the data? • Are you using data someone else produced? If so, where is it from?	• Focus groups and interviews with practitioners and experts. • OMCs data • Piloting and testing generated data All data is collected inside the organization; thus, no external data is used
What types of data do you expect to be processed / generated? Please refer to both special categories of personal data and non-special categories.	Code number (identifying the victim), medical data (BP, HR, RR), text, numbers and optional geolocation metadata or photos
Please explain the relation of the data processing/generation (for each data type) to the objectives of the project.	All data processed by EKAB in the framework of the project will facilitate the triage process.
How will you be processing the data? Provide separate answers for each data type/category you will be processing, collecting, or generating.	Code number randomly generated by the triage process (device) and medical data will be exported by the device (optional use of sensors)
For each data type, please state the format(s) in which you expect that type of data to be collected/generated. For example, numerical data, image data, text sequences, audio data etc.	Numerical data, image data, text sequences, audio data
For each type of data what is the expected size?	Manageable size (bytes-kilobytes) except for image data, which is expected to be of megabyte-gigabyte size

Data Management Procedures	
Does your organization have data management guidelines? If so, what are they?	Yes. Data management guidelines are related to the collection, access, analysis and storage procedures which best serve to comply with GDPR guidelines for protection of personal data processed at EKAB. EKAB collects and processes the Personal Data of individuals affected by Humanitarian Emergencies in order to perform humanitarian activities. Consent for the processing of data is central to the GDPR's guidelines. The beneficiaries are informed of why each piece of personal data is necessary for

	the provision of services and how this data will be processed. Also, they must be informed of their rights regarding the data collected.
Does your organization have a data protection or security policy that you will follow? If so, what is it?	Data Protection Guidelines have been developed by the EKAB DPO and concern: Technical Security Measures: 1.Password Protection 2. Encryption 3. Antivirus 4. Systems Backup 5. Government Cloud Computing Service (GCloud) 6. Automatic Logout 7. Data Access Control Operational Procedures for every service (software, hardware)
Does your organization have a Research Data Management policy? What is it?	EKAB has developed a data management plan which is adjusted at every research proposal if any research data are to be collected or used. The plan covers data types and volume, capture, storage, integrity, confidentiality, retention and destruction, sharing and deposit.
Are there any formal standards you will adopt when processing data for the project?	Yes, data processing will be examined according to the requirements
Please provide the contact details of your organization's DPO.	Contact Person: Apostolos Skarlis Phone: +30213.214.3444 Mobile:+306975.166.166 Email: dpo@ekab.gr

Documentation, Organization and Storage	
Who will be responsible for documentation, organization, and storage?	EKAB's IT department
How will you label and organize data, records, and files?	Using EKAB's guidelines that are in compliance with GDPR. The key is that data subjects receive a unique code according to which data will be labeled and organized Unique code and name will be organized separately from other data.
How long will you be storing personal data generated in the project for?	5 years
How and where will the data be stored?	Will be stored in electronic format on the developed system or if needed on server or cloud
Are you using proprietary file formats to generate and store your research data? If so, will the	No

documentation about the software needed to access the data be included?	
If data are collected with mobile devices, how will you transfer and store the data?	Bluetooth protocol, wifi and 4G -5G network
If data are held in various places, how will you keep track of versions?	By numbering and dating the relevant versions.

Access	
Who within your organization will manage access to this data?	EKAB's IT Department under Medical Services
Who within your organization will have access to the data processed for the iProcureSecurity PCP project?	IT department and the team participating to the project
How will the identity of the person accessing the data be ascertained?	By using personal login account with password.
Will there by conditions to gaining data access? If so, what will those conditions be?	No, there is a securing entry to accessing data due to the structured cabling of EKAB's network
What methods or software tools will be needed to access the data? Will any other accompanying information be required to properly interpret the data?	Web browser, Microsoft office suite No
What information, if any needs to be retained in order for the data to be read and interpreted in the future?	Information related to the reporting of the project
Will any data be made openly available for all project partners?	Only to the partners with which EKAB will collaborate, or to the other members of the consortium if needed
How will the data that is made openly available be maintained? In a repository?	Yes, in a repository

Sharing	
What data will be shared?	Code number (identifying the victim), medical data (BP, HR, RR), text, numbers and optional geolocation metadata or photos
When will data be shared?	Throughout the different phases of the response in case of an emergency (scenario)
For what purposes of the project will data be shared?	To facilitate the interoperability of different components To make informed decisions To serve the best of interest of the data subject
Who will data be shared with?	Involved parties in the scenario.
Does sharing raise any privacy, ethical, or confidentiality concerns? If yes, what are they and why?	No

Will a data sharing agreement be required? If some data categories and types are kept closed provide a rationale for doing so.	Yes

Security	
What are the major risks to data security?	1.Accidental exposure of data 2.Phishing of data 3.Data loss in the server or/and cloud
How will each of these risks be managed?	1.Intensive relevant trainings, unique strong passwords of users 2. Strong antivirus system and encryption of data 3. Regular backing up of the data to another location 4. Data will be shared encrypted
Do you need to anonymize any of the data?	If there is sensitive personal data should be anonymized
What security measures do you anticipate being required for safe data storage, sharing and management?	1.Password Protection (high secure passwords that change regularly) 2. Encryption 3. Antivirus 4. Systems Backup 5. Data Access Control 6.Operational Procedures (software, hardware)
Have you implemented or outlined any procedures to follow in the case of a data breach? If so, what are they?	In case of data breach, data users a) Report to the EKAB's DPO to assess the break b) Change passwords and c) Inform the data subject
Are your digital and non-digital data, and any copies, held in a safe and secure location?	Yes. Non digital data in cupboards that are locked Digital data in the EKAB's server and cloud. EKAB account password is required to accessing them

Ethical Considerations	
What types of special category personal data do you intend to generate/process?	Code number (identifying the victim), medical data (BP, HR, RR), text, numbers and optional geolocation metadata or photos
Will any of the data subjects be children?	No
Will any of the data subjects be vulnerable people?	No
Will you be collecting personal or sensitive data from people who have not given their explicit consent to participate in the Project?	No
For each category of data you intend to collect, please provide: • If the data is personal data, as defined by the GDPR, which of the six Art. 6 bases will you rely	• the data subject has given consent to the processing of his or her personal data for one or more specific purposes • the data subject has given explicit consent to the processing of those personal data for one or more specified purposes,

on for the processing of each category of personal data? • If the data is sensitive data, as defined by the GDPR, which of the ten Art. 9 bases will you rely on for the processing of each category of sensitive data?	except where Union or Member State law provide that the prohibition referred to Article 9, in paragraph 1 of GDPR, may not be lifted by the data subject
Have you already gained consent for data preservation and sharing from any data subject(s)?	Yes
Will you engage in large scale or big data processing?	No
Will any entity (including any service provider) outside of the E.U. have access to personal or sensitive data? If so, who? For what purpose? Where is each of these entities located?	Project partners AAHD and IBB from Turkey. Purpose: project activities such as OMC, webinar events, triage management system requirements, use cases.

IZMIR BUYUKSEHIR BELEDIYESI, IBB

Table 11: **IBB DMP Questionnaire**

Data Description	
What type of data will you collect? Please provide in brief.	IBB will provide Open Market Consultation, that's why SME, Industry and previous projects will be collected. But this information is available in the web page (public available information). AAHD will provide questionnaires containing use cases and processes via google forms. That does not have personal questions.
What is the purpose of the data collection?	The purpose of the data collection is to reach the relevant institutions, experts, projects, events to raise awareness on the project and important activities like OPM.
Please explain: • What is the origin of the data? • Are you using data someone else produced? If so, where is it from?	Publicly available data IBB will not use data that produced by someone else
What types of data do you expect to be processed / generated? Please refer to both special categories of personal data and non-special categories.	Data from the collected responses; medical procedures, ways of communication, algorithms, medical equipment, trainings.

Please explain the relation of the data processing/generation (for each data type) to the objectives of the project.	To prepare a relevant and beneficent OMC.
How will you be processing the data? Provide separate answers for each data type/category you will be processing, collecting, or generating.	The collected data will be used for scientific purposes; to test the reliability, validity, sensitivity, specificity of the products for triage management system.
For each data type, please state the format(s) in which you expect that type of data to be collected/generated. For example, numerical data, image data, text sequences, audio data etc.	Data will be collected mainly numerically.
For each type of data what is the expected size?	<1MB

Data Management Procedures	
Does your organization have data management guidelines? If so, what are they?	According to the DMP
Does your organization have a data protection or security policy that you will follow? If so, what is it?	According to the DMP
Does your organization have a Research Data Management policy? What is it?	According to the DMP
Are there any formal standards you will adopt when processing data for the project?	According to the DMP
Please provide the contact details of your organization's DPO.	Prm. Onur Karaot onurkaraot@gmail.com

Documentation, Organization and Storage	
Who will be responsible for documentation, organization, and storage?	Technical Manager
How will you label and organize data, records, and files?	All data will be labeled with the project acronym and a unique name and version number (where necessary).
How long will you be storing personal data generated in the project for?	For the duration of the project.
How and where will the data be stored?	Internal policies, confidentiality agreements, secured storage of documents where only authorized access is allowed, password-protected access to personal computers and to databases
Are you using proprietary file formats to generate and store your research data? If so, will the documentation about the software needed to access the data be included?	Yes, xls.
If data are collected with mobile devices, how will you transfer and store the data?	N/A
If data are held in various places, how will you keep track of versions?	N/A

Access	

Who within your organization will manage access to this data?	Technical Manager
Who within your organization will have access to the data processed for the iProcureSecurity PCP project?	Technical Manager
How will the identity of the person accessing the data be ascertained?	Password protection
Will there by conditions to gaining data access? If so, what will those conditions be?	N/A
What methods or software tools will be needed to access the data? Will any other accompanying information be required to properly interpret the data?	Microsoft Office No
What information, if any needs to be retained in order for the data to be read and interpreted in the future?	N/A
Will any data be made openly available for all project partners?	Project partners will have access and contribute to all types of collected data mentioned above.
How will the data that is made openly available be maintained? In a repository?	GDPR compliant collaboration software

Sharing	
What data will be shared?	As mentioned above.
When will data be shared?	During the project lifetime
For what purposes of the project will data be shared?	Awareness for the project activities (e.g. OMCs, call for tender, observer and expert board) and retrieving expert opinion and feedback
Who will data be shared with?	Project partners only
Does sharing raise any privacy, ethical, or confidentiality concerns? If yes, what are they and why?	No
Will a data sharing agreement be required? If some data categories and types are kept closed provide a rationale for doing so.	No

Security	
What are the major risks to data security?	None, all collected information is publicly available
How will each of these risks be managed?	N/A
Do you need to anonymize any of the data?	N/A
What security measures do you anticipate being required for safe data storage, sharing and management?	Internal policies, confidentiality agreements, secured storage of documents where only authorized access is allowed, password-protected access to personal computers and to databases
Have you implemented or outlined any procedures to follow in the case of a data breach? If so, what are they?	According to GDPR Art. 33, 34
Are your digital and non-digital data, and any copies, held in a safe and secure location?	Yes

Ethical Considerations	
What types of special category personal data do you intend to generate/process?	N/A
Will any of the data subjects be children?	NO
Will any of the data subjects be vulnerable people?	NO
Will you be collecting personal or sensitive data from people who have not given their explicit consent to participate in the Project?	NO
For each category of data you intend to collect, please provide: • If the data is personal data, as defined by the GDPR, which of the six Art. 6 bases will you rely on for the processing of each category of personal data? • If the data is sensitive data, as defined by the GDPR, which of the ten Art. 9 bases will you rely on for the processing of each category of sensitive data?	Art 6 GDPR 1.a
Have you already gained consent for data preservation and sharing from any data subject(s)?	Informed consent will be signed before the pilots Workshops/Focus Groups
Will you engage in large scale or big data processing?	NO
Will any entity (including any service provider) outside of the E.U. have access to personal or sensitive data? If so, who? For what purpose? Where is each of these entities located?	IBB is form Turkey

KENTRO MELETON ASFALEIAS, KEMEA

Table 12: **KEMEA DMP Questionnaire**

Data Description	
What type of data will you collect? Please provide in brief.	Stakeholder's data participating in the events, , data of state of the art technologies, requirements of triage management system, software, software data, literature, images, audio files, deliverables, questionnaires, solutions overview, OMC Webinars data, Call for Tenders documentation, Call for Tenders applicants' data, Framework Agreement (including IPR and Data Processing Agreement), phase Contracts .

What is the purpose of the data collection?	The purpose of the data collection is: - Data processing for project management and coordination - Open Market Consultation (OMC) or other webinar events, in which participants' personal data may be processed, while participants may be asked to respond to questions related to the market. - Data processing during the research activities: Interviews/questionnaires - Data processing during the research activities: Trials - Pre-Commercial Procurement
Please explain: • What is the origin of the data? • Are you using data someone else produced? If so, where is it from?	Publicly available data or Primary data, questionnaires filled out by the suppliers, information from UOG members and public buyers (procurers).Personal data will be collected from the data subjects themselves.
What types of data do you expect to be processed / generated? Please refer to both special categories of personal data and non-special categories.	Data to be processed: a) personal data (names, contact details, images, voices) of participants in the OMC events, b)information of state of art technologies through OMC questionnaires, c) data of contractors as part of the procurement process.
Please explain the relation of the data processing/generation (for each data type) to the objectives of the project.	The data processing is required in order to implement webinar events, OMC, and prepare, launch and implement the PCP procurement and pilots. The data will be used for the purpose of the project only.
How will you be processing the data? Provide separate answers for each data type/category you will be processing, collecting, or generating.	Collected data will be stored safely in KEMEA's local servers, will be used for the needs of the project's management, they will be shared with partners only for the project's needs and will be deleted after 5 years from the end of the project.
For each data type, please state the format(s) in which you expect that type of data to be collected/generated. For example, numerical data, image data, text sequences, audio data etc.	Personal data, literature, questionnaires in Text format, Requirements of triage management system in xls, images, videos in audiofiles.
For each type of data what is the expected size?	To be determined at a later stage

Data Management Procedures	

Does your organization have data management guidelines? If so, what are they?	KEMEA follows EC's relevant guidelines.
Does your organization have a data protection or security policy that you will follow? If so, what is it?	KEMEA applies a data protection policy and a security policy (internal documents, written in Greek) Please see: http://www.kemea.gr/en/kemea/terms-of-use-privacy-policy-personal-data-protection for KEMEA's publicly available policy.
Does your organization have a Research Data Management policy? What is it?	No, KEMEA follows EC's relevant guidelines and researchers' codes of Conduct (e.g. ALLEA)
Are there any formal standards you will adopt when processing data for the project?	According to KEMEA's data protection policy.
Please provide the contact details of your organization's DPO.	Data Protection Officer (DPO) Center for Security Studies (KEMEA) Hellenic Ministry of Citizen Protection P. Kanellopoulou 4, 101 77 Athens, Greece Tel: +30 2107710805 (ext. 384) www.kemea.gr dpo@kemea-research.gr

Documentation, Organization and Storage	
Who will be responsible for documentation, organization, and storage?	The Project Manager
How will you label and organize data, records, and files?	Digital files, labeled with project's acronym and file name and version number.
How long will you be storing personal data generated in the project for?	Until the end of the project and no later than 5 years after the end of the project according to the Grant Agreement for keeping records that can be reviewed/checked by the EC.
How and where will the data be stored?	The data will be stored in electronic format on KEMEA server, password protected.
Are you using proprietary file formats to generate and store your research data? If so, will the documentation about the software needed to access the data be included?	Not applicable
If data are collected with mobile devices, how will you transfer and store the data?	Not applicable
If data are held in various places, how will you keep track of versions?	Not applicable

Access	
Who within your organization will manage access to this data?	The Project Manager
Who within your organization will have access to the data processed for the iProcureSecurity PCP project?	The Project Manager
How will the identity of the person accessing the data be ascertained?	The data will be password protected.

Will there by conditions to gaining data access? If so, what will those conditions be?	Not applicable
What methods or software tools will be needed to access the data? Will any other accompanying information be required to properly interpret the data?	MS Office tools
What information, if any needs to be retained in order for the data to be read and interpreted in the future?	Not applicable
Will any data be made openly available for all project partners?	All the project partners have access to the data through a share drive.
How will the data that is made openly available be maintained? In a repository?	Within a secure repository, taking full care of them and in full respect of the GDPR and legislation

Sharing	
What data will be shared?	As described in previous sections.
When will data be shared?	During the project life-cycle.
For what purposes of the project will data be shared?	The data will be shared for project's implementation activities: Open Market Consultation, Procurement, Use cases, and UOG contribution.
Who will data be shared with?	Consortium
Does sharing raise any privacy, ethical, or confidentiality concerns? If yes, what are they and why?	No
Will a data sharing agreement be required? If some data categories and types are kept closed provide a rationale for doing so.	No

Security	
What are the major risks to data security?	Major risks: Viruses, Data phishing, Data loss, Data breach (confidentiality, availability)
How will each of these risks be managed?	According to KEMEA's security policy.
Do you need to anonymize any of the data?	No
What security measures do you anticipate being required for safe data storage, sharing and management?	Password protection, access limited to staff involved.
Have you implemented or outlined any procedures to follow in the case of a data breach? If so, what are they?	Yes, there is a particular policy to be activated in case of a data breach (part of data protection policy) with specific forms to be filled.
Are your digital and non-digital data, and any copies, held in a safe and secure location?	Yes. KEMEA implements a series of measures, indicatively: 1) Data Protection Policy 2) Data erasure/destruction policy 3) "Clean-desk" policy

	4) Data breach form 5) Terms of use- Privacy Policy – Data Protection for KEMEA's websites 6) Data Subject's Communication form 7) Cookies Policy 8) Information Security Policy 9) Roles and responsibilities of security 10) Census and monitoring of IT tools 11) Business Continuity 12) Access control to networks and systems 13) Security of interfaces 14) Authorised access to the CED and offices 15) Network and system integrity 16) Authentication 17) Defense

Ethical Considerations	
What types of special category personal data do you intend to generate/process?	Voice of partners/participants in recorded webinar
Will any of the data subjects be children?	Not applicable
Will any of the data subjects be vulnerable people?	Not applicable
Will you be collecting personal or sensitive data from people who have not given their explicit consent to participate in the Project?	No
For each category of data you intend to collect, please provide: • If the data is personal data, as defined by the GDPR, which of the six Art. 6 bases will you rely on for the processing of each category of personal data? • If the data is sensitive data, as defined by the GDPR, which of the ten Art. 9 bases will you rely on for the processing of each category of sensitive data?	• Art. 6 par. 1(a) consent (from webinar and interviews participants and for partners' images and voice) • Art. 6 par. 1(b) contract (for partners' names and contact details) • Art. 9 par. 2 (a) consent (for webinar participants' voice).
Have you already gained consent for data preservation and sharing from any data subject(s)?	To be determined at a later stage.
Will you engage in large scale or big data processing?	No
Will any entity (including any service provider) outside of the E.U. have access to personal or sensitive data? If so, who? For what purpose? Where is each of these entities located?	Project partners AAHD and IBB from Turkey. Purpose: project activities such as OMC, webinar events, triage management system requirements, use cases.

ACIL AFET AMBULANS HEKIMLERI DERNEGI, AAHD

Table 13: **AAHD DMP Questionnaire**

Data Description	

What type of data will you collect? Please provide in brief.	AAHD will provide Open Market Consultation, that's why SME, Industry and previous projects will be collected. But this information is available in the web page (public available information). AAHD will provide questionnaires containing use cases and processes via google forms. That does not have personal questions.
What is the purpose of the data collection?	The purpose of the data collection is to reach the relevant institutions, experts, projects, events to raise awareness on the project and important activities like OPM.
Please explain: • What is the origin of the data? • Are you using data someone else produced? If so, where is it from?	Publicly available data, Uses cases created by AAHD AAHD will not use data that produced by someone else
What types of data do you expect to be processed / generated? Please refer to both special categories of personal data and non-special categories.	Data from the collected responses; medical procedures, ways of communication, algorithms, medical equipment, trainings.
Please explain the relation of the data processing/generation (for each data type) to the objectives of the project.	To prepare a relevant and beneficent OMC. AAHD is the leader of WP8; so, collect data that will be generated from the evaluation of procurer pilots. These data will not contain personal data. Before all the pilot testing each partner that will host the pilot will get an Ethical approval. Consent forms will be open for signature before the pilots. The consent forms will be removed by the conclusion of the iProcureSecurity PCP Project. Vital signs, mechanism of injury, age, gender and medical history will be created for use cases. All of these will be simulated cases. The response time; triage colors, treatment, means of transport, hospital selection, stake holders will be selected for each case to test the triage management solutions. To understand under-over triage rates for example.
How will you be processing the data? Provide separate answers for each data type/category you will be processing, collecting, or generating.	The collected data will be used for scientific purposes; to test the reliability, validity, sensitivity, specificity of the products for triage management system.

For each data type, please state the format(s) in which you expect that type of data to be collected/generated. For example, numerical data, image data, text sequences, audio data etc.	Data will be collected mainly numerically.
For each type of data what is the expected size?	<1MB

Data Management Procedures	
Does your organization have data management guidelines? If so, what are they?	According to the DMP
Does your organization have a data protection or security policy that you will follow? If so, what is it?	According to the DMP
Does your organization have a Research Data Management policy? What is it?	According to the DMP
Are there any formal standards you will adopt when processing data for the project?	According to the DMP
Please provide the contact details of your organization's DPO.	Dr. Melih Gunduz melihgunduz@gmail.com

Documentation, Organization and Storage	
Who will be responsible for documentation, organization, and storage?	Project Manager
How will you label and organize data, records, and files?	All data will be labeled with the project acronym and a unique name and version number (where necessary).
How long will you be storing personal data generated in the project for?	For the duration of the project.
How and where will the data be stored?	Internal policies, confidentiality agreements, secured storage of documents where only authorized access is allowed, password-protected access to personal computers and to databases
Are you using proprietary file formats to generate and store your research data? If so, will the documentation about the software needed to access the data be included?	Yes, xls.
If data are collected with mobile devices, how will you transfer and store the data?	N/A
If data are held in various places, how will you keep track of versions?	N/A

Access	
Who within your organization will manage access to this data?	Project Manager

Who within your organization will have access to the data processed for the iProcureSecurity PCP project?	Project Manager
How will the identity of the person accessing the data be ascertained?	Password protection
Will there by conditions to gaining data access? If so, what will those conditions be?	N/A
What methods or software tools will be needed to access the data? Will any other accompanying information be required to properly interpret the data?	Microsoft Office No
What information, if any needs to be retained in order for the data to be read and interpreted in the future?	N/A
Will any data be made openly available for all project partners?	Project partners will have access and contribute to all types of collected data mentioned above.
How will the data that is made openly available be maintained? In a repository?	GDPR compliant collaboration software

Sharing	
What data will be shared?	As mentioned above.
When will data be shared?	During the project lifetime
For what purposes of the project will data be shared?	Awareness for the project activities (e.g. OMCs, call for tender, observer and expert board) and retrieving expert opinion and feedback
Who will data be shared with?	Project partners only
Does sharing raise any privacy, ethical, or confidentiality concerns? If yes, what are they and why?	No
Will a data sharing agreement be required? If some data categories and types are kept closed provide a rationale for doing so.	No

Security	
What are the major risks to data security?	None, all collected information is publicly available
How will each of these risks be managed?	N/A
Do you need to anonymize any of the data?	N/A
What security measures do you anticipate being required for safe data storage, sharing and management?	Internal policies, confidentiality agreements, secured storage of documents where only authorized access is allowed, password-protected access to personal computers and to databases
Have you implemented or outlined any procedures to follow in the case of a data breach? If so, what are they?	According GDPR Art. 33, 34

Are your digital and non-digital data, and any copies, held in a safe and secure location?	Yes

Ethical Considerations	
What types of special category personal data do you intend to generate/process?	N/A
Will any of the data subjects be children?	NO
Will any of the data subjects be vulnerable people?	NO
Will you be collecting personal or sensitive data from people who have not given their explicit consent to participate in the Project?	NO
For each category of data you intend to collect, please provide: • If the data is personal data, as defined by the GDPR, which of the six Art. 6 bases will you rely on for the processing of each category of personal data? • If the data is sensitive data, as defined by the GDPR, which of the ten Art. 9 bases will you rely on for the processing of each category of sensitive data?	Art 6 GDPR 1.a
Have you already gained consent for data preservation and sharing from any data subject(s)?	Informed consent will be signed before the pilots Workshops/Focus Groups
Will you engage in large scale or big data processing?	NO
Will any entity (including any service provider) outside of the E.U. have access to personal or sensitive data? If so, who? For what purpose? Where is each of these entities located?	AAHD is from Turkey

EMPIRICA GESELLSCHAFT FUR KOMMUNIKATIONS UND TECHNOLOGIEFORSCHUNG MBH, EMPIRICA

Table 14: **EMPIRICA DMP Questionnaire**

Data Description	
What type of data will you collect? Please provide in brief.	As WP3 lead, empirica is mainly involved in the OMC process in the PCP and is therefore expected to collect OMC-related data, such as personal contact data through event registrations (mostly using online forms),

	feedback by potential suppliers through an online survey and email. In later phases of the PCP, empirica may support the definition of data to be collected during the piloting of the solutions but is not expected to access or process that data. Further data can be collected by empirica from project partners, e.g. related to their exploitation plans in WP8.
What is the purpose of the data collection?	The purpose of the data collection is to facilitate the OMC process and ensure that potential suppliers are invited to relevant events and opportunities of sharing and receiving information about the project.
Please explain: • What is the origin of the data? • Are you using data someone else produced? If so, where is it from?	Most data is produced and kept centrally, as for most events, the registration and communication is handled by the project coordinator SYNYO. empirica as a beneficiary receives access to that stored information via the project's central repository used and provided by SYNYO (Google Drive) and can use it in subsequent reports, such as D3.1 Report on the Open Market Consultation.
What types of data do you expect to be processed / generated? Please refer to both special categories of personal data and non-special categories.	Types of data expected to be processed are: personal information (first name, last name, email, organisation, country of residence, type of organisation (public, private, SME, large enterprise)), information about available products and services as part of an OMC questionnaire.
Please explain the relation of the data processing/generation (for each data type) to the objectives of the project.	Data processing is necessary to ensure that the objective of the project related to organising OMC events is met. Data will not be used for other purposes outside of the scope of the project.
How will you be processing the data? Provide separate answers for each data type/category you will be processing, collecting, or generating.	Only empirica staff members with access to the central project repository may access the data. The personal information will be used to send invitations and reminders for the OMC events, and other related invitations (e.g. for providing information for the pitching session planned in the international OMC). The information about products and services is processed as part of D3.1. As D3.1 is a public report, no personal information will be reported.
For each data type, please state the format(s) in which you expect that type of data to be collected/generated. For example, numerical data, image data, text sequences, audio data etc.	Personal data captured in spreadsheets (.csv, .xlsm, xlsb, xlsx) as text

For each type of data what is the expected size?	<10 MB

Data Management Procedures	
Does your organization have data management guidelines? If so, what are they?	See https://empirica.com/special-pages/privacy-statement
Does your organization have a data protection or security policy that you will follow? If so, what is it?	See https://empirica.com/special-pages/privacy-statement
Does your organization have a Research Data Management policy? What is it?	No specific policy in place
Are there any formal standards you will adopt when processing data for the project?	See https://empirica.com/special-pages/privacy-statement
Please provide the contact details of your organization's DPO.	As a private research company, we mainly process client data and data for research projects, therefore no official DPO is required for this (see here).

Documentation, Organization and Storage	
Who will be responsible for documentation, organization, and storage?	empirica staff working on the project. For a current list, consult the central project staff contact database.
How will you label and organize data, records, and files?	We use only digital files, organised in folders belonging to the iProcureSecurity PCP tree
How long will you be storing personal data generated in the project for?	Typically, up to four years after project completion.
How and where will the data be stored?	empirica uses a cloud service provided by Deutsche Telekom that uses its own business space (tenant) accessible only to empirica staff. Servers are located in Germany. All project relevant data is stored in the central project repository (Google Drive) managed by the project coordinator. A specific team (MS Teams) is used to store a copy of that data.
Are you using proprietary file formats to generate and store your research data? If so, will the documentation about the software needed to access the data be included?	No
If data are collected with mobile devices, how will you transfer and store the data?	Not applicable
If data are held in various places, how will you keep track of versions?	Not applicable

Access	
Who within your organization will manage access to this data?	empirica staff working on the project. For a current list, consult the central project staff contact database.

Who within your organization will have access to the data processed for the iProcureSecurity PCP project?	empirica staff working on the project. For a current list, consult the central project staff contact database.
How will the identity of the person accessing the data be ascertained?	MS Teams allows for clear identification of staff members.
Will there by conditions to gaining data access? If so, what will those conditions be?	Access to the project team on MS Teams is decided by the company directors based on the team required to carry out the project.
What methods or software tools will be needed to access the data? Will any other accompanying information be required to properly interpret the data?	MS Office tools
What information, if any needs to be retained in order for the data to be read and interpreted in the future?	Not applicable
Will any data be made openly available for all project partners?	All project-related data is stored in the central project repository. No further data held by empirica is planned to be shared with the project partners.
How will the data that is made openly available be maintained? In a repository?	Not applicable

Sharing	
What data will be shared?	No data pertaining to empirica's work in the project will be shared outside of the project consortium.
When will data be shared?	Not applicable
For what purposes of the project will data be shared?	Not applicable
Who will data be shared with?	Not applicable
Does sharing raise any privacy, ethical, or confidentiality concerns? If yes, what are they and why?	Not applicable
Will a data sharing agreement be required? If some data categories and types are kept closed provide a rationale for doing so.	Not applicable

Security	
What are the major risks to data security?	Data breach, viruses
How will each of these risks be managed?	Use of external support through the provider
Do you need to anonymize any of the data?	No
What security measures do you anticipate being required for safe data storage, sharing and management?	Processes in place like 2FA, password protection, access limited only to relevant staff working on the project, internal briefing about best practices in storing, sharing and managing data.

Have you implemented or outlined any procedures to follow in the case of a data breach? If so, what are they?	No specific procedures in place.
Are your digital and non-digital data, and any copies, held in a safe and secure location?	Yes

Ethical Considerations	
What types of special category personal data do you intend to generate/process?	Not applicable
Will any of the data subjects be children?	Not applicable
Will any of the data subjects be vulnerable people?	Not applicable
Will you be collecting personal or sensitive data from people who have not given their explicit consent to participate in the Project?	No
For each category of data you intend to collect, please provide: • If the data is personal data, as defined by the GDPR, which of the six Art. 6 bases will you rely on for the processing of each category of personal data? • If the data is sensitive data, as defined by the GDPR, which of the ten Art. 9 bases will you rely on for the processing of each category of sensitive data?	For OMC-related data empirica uses data already provided through forms owned by other partners, e.g. SYNYO, therefore Art. 6 para.1 lit. a General Data Protection Regulation applies. In all other cases in which empirica is approached in relation to the project and processes data Art. 6 para. 1 lit. f General Data Protection Regulation applies.
Have you already gained consent for data preservation and sharing from any data subject(s)?	No
Will you engage in large scale or big data processing?	No
Will any entity (including any service provider) outside of the E.U. have access to personal or sensitive data? If so, who? For what purpose? Where is each of these entities located?	No

2.1.4 What type of information will be considered as public, restricted or confidential following the "Guidance Guidelines for the classification of research results" of the European Commission

The following table presents a description and classification of iProcureSecurity PCP deliverables.

Table 15: **iProcureSecurity PCP Deliverables**

Deliverable Number	Deliverable Title	Dissemination Level

D1.1	Kick-off meeting report	Confidential, only for members of the consortium (including the Commission Services)
D1.2	Data Management Plan	Public
D1.3	Progress report	Confidential, only for members of the consortium (including the Commission Services)
D1.4	Final project documentation	Confidential, only for members of the consortium (including the Commission Services)
D1.5	Data Management Plan Update I	Public
D1.6	Data Management Plan Update II	Public
D2.1	Requirements for Triage Management Systems for Emergency Medical Services	Public
D2.2	Use cases and process models for Triage Management Systems for Emergency Medical Services (v1)	Confidential, only for members of the consortium (including the Commission Services)
D2.3	Final use cases and process models for Triage Management Systems for EMS	Public
D3.1	Report on the Open Market Consultation	Public
D3.2	Tender documents	Public
D3.3	Tender platform and evaluation system development report	Public
D4.1	Call for Tenders results	Confidential, only for members of the consortium (including the Commission Services)
D5.1	Phase I results	Confidential, only for members of the consortium (including the Commission Services)
D6.1	Phase II results	Confidential, only for members of the consortium (including the Commission Services)
D7.1	Phase III results	Confidential, only for members of the consortium (including the Commission Services)
D8.1	Methods for prototype tests	Public
D8.2	Evaluation framework for iProcureSecurity PCP	Public
D8.3	Interim report on exploitation and procurement planning	Confidential, only for members of the consortium (including the Commission Services)
D8.4	iProcureSecurity PCP exploitation and procurement plans	Confidential, only for members of the consortium (including the Commission Services)
D8.5	iProcureSecurity PCP Pilot Outcomes	Public
D9.1	Project website, social media channels and communication activities	Public
D9.2	Dissemination & communication plan	Public
D9.3	Dissemination package 1	Public
D9.4	Dissemination package 2	Public
D9.5	Dissemination package 3	Public
D9.6	Symposium summary	Public

D10.1	H - Requirement No. 1	Confidential, only for members of the consortium (including the Commission Services)
D10.2	POPD - Requirement No. 2	Confidential, only for members of the consortium (including the Commission Services)
D10.3	H - Requirement No. 4	Confidential, only for members of the consortium (including the Commission Services)
D10.4	GEN - Requirement No. 5	Confidential, only for members of the consortium (including the Commission Services)
D10.5	GEN - Requirement No. 6	Confidential, only for members of the consortium (including the Commission Services)
D10.6	GEN - Requirement No. 7	Confidential, only for members of the consortium (including the Commission Services)
D10.7	GEN - Requirement No. 8	Confidential, only for members of the consortium (including the Commission Services)

2.2 Fair Data

According to the H2020 Guidelines on FAIR Data Management[1] each project should provide information on:

- How research data are handled during and after the end of the project;
- Which data are collected, processed and/or generated;
- Which methodology and standards are applied;
- Whether the data are shared/made open access, and
- How data are curated and preserved after the project end.

These guidelines help Horizon 2020 beneficiaries to make research data findable, accessible, interoperable and reusable (FAIR), to ease knowledge discovery and innovation and to allow data and knowledge integration and reuse.

To this end, the consortium will follow the conditions, rules and regulations from the ZENODO repository to ensure compliance with FAIR principles:

- The relevant Task Leader should collect the data in the most suitable format, store and make findable any data catalogued as openly accessible in the ZENODO repository. A table has been developed to facilitate partners in case they have data that can be made available (see Annex I).
- Ensure that research outputs and data sets are cross-referencing each other (e.g. publications and the data behind them).
- Outline the discoverability of the data; i.e.: give metadata provision (author, date of publication, etc.)

[1] http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

- Data will be made accessible within one month of publishing the data, unless the responsible partner has outlined justifiable reasons to keep the data confidential.
- Each partner is responsible for their records and documentation in relation to data generated, which must be in line with this DMP and overseen by Task leads.
- After uploading data in ZENODO, Task Leaders should inform the DMP Responsible (KEMEA for their follow-up).

In addition, the partners must take measures to ensure that data is backed-up using reliable methods.

2.2.1 Making data findable, including provisions for metadata

According to the iProcureSecurity PCP Grant Agreement section 29.3, open access to research data is applicable. Thus, the FAIR principle refers to scientific publications, research results (i.e. from surveys etc.), dissemination material as well as digital research data.

According to section 29.3 of the Grant Agreement, regarding the digital research data generated in the action ('data'), the consortium partners must:

(a) deposit in a research data repository and take measures to make it possible for third parties to access, mine, exploit, reproduce and disseminate — free of charge for any user — the following:
(i) the data, including associated metadata, needed to validate the results presented in scientific publications, as soon as possible;
(ii) other data, including associated metadata, as specified and within the deadlines laid down in the 'data management plan';
(b) provide information — via the repository — about tools and instruments at the disposal of the beneficiaries and necessary for validating the results (and — where possible — provide the tools and instruments themselves).
This does not change the obligation to protect results in Article 27 of the Grant Agreement, the confidentiality obligations in Article 36, the security obligations in Article 37 or the obligations to protect personal data in Article 39, all of which still apply. As an exception, the consortium partners do not have to ensure open access to specific parts of their research data under Point (a)(i) and (iii), if the achievement of the action's main objective would be jeopardised by making those specific parts of the research data openly accessible. In this case, the DMP must contain the reasons for not giving access.

One of the goals of iProcureSecurity PCP is related to the findability of the data by making sure that the generated data will be identifiable and easily discoverable. To this end, the datasets will be accompanied with rich metadata in order to increase their findability. The creation of these metadata –where appropriate- will be based on the OpenAIRE2 guidelines for Data Archives. OpenAIRE has adopted the DataCite Metadata Schema v3.1 and apart from a Digital Object Identifier (DOI), accepts also other persistent identifier schemes, such as Archival Resource Key (ARK), Handle, Persistent Uniform Resource Locator (PURL), Uniform Resource Name (URN) and Uniform Resource Locator (URL). Non-confidential data gathered during the project will be compiled and deposited in OpenAIRE's Zenodo repository to ensure discoverability, accessibility, and intelligibility.

[2] https://guidelines.openaire.eu/en/latest/data/index.html

2.2.2 Making data accessible

One of the goals of iProcureSecurity PCP is related to the findability of the data by making sure that the generated data will be identifiable and easily discoverable. To this end, the datasets will be accompanied with rich metadata in order to increase their findability. The creation of these metadata –where appropriate- will be based on the OpenAIRE3 guidelines for Data Archives. OpenAIRE has adopted the DataCite Metadata Schema v3.1 and apart from a Digital Object Identifier (DOI), accepts also other persistent identifier schemes, such as Archival Resource Key (ARK), Handle, Persistent Uniform Resource Locator (PURL), Uniform Resource Name (URN) and Uniform Resource Locator (URL). Non-confidential data gathered during the project will be compiled and deposited in OpenAIRE's Zenodo repository to ensure discoverability, accessibility, and intelligibility.

2.2.3 Making data accessible

The iProcureSecurity PCP project deliverables will be accessible to the authorised partners through the project common online collaborative tool (https://drive.google.com/). All the information related to these deliverables will be available by work package and task following a standardized format.

The public project deliverables along with the executive summaries of deliverables which are not public, will be available in the project's official website.

In more detail, the deliverables that have been defined in the Description of Action as 'Public' will be provided with an open space on the project website after their review and approval by the EC, so that anyone can access them. Regarding the deliverables which are confidential, and their content is restricted only to members of the consortium, an executive summary of the deliverable will be available in the project website after the EC approval as well.

More information on the variety of channels and materials that have been employed by the project in order to enhance its footprint and reinforce data accessibility can be found in the relevant deliverable D9.2 Dissemination & Communication Plan (PU). The latter indicates the communication and dissemination channels which consist of:

- A dissemination toolkit which comprises leaflets, brochures, factsheets, posters and roll-up banners.
- The creation and distribution of newsletters, factsheets and booklets to promote events and keep the wide audience of the project informed on the activities and events.
- Scientific papers to high impact journals.
- Participation in Conferences, Exhibitions and Workshops.
- Videos that will be created to advertise the project's achievements.
- The project's website.
- The extended use of social media campaigns in order to engage and interact with the projects' stakeholders.
- Synergies with existing and new EU-funded projects and initiatives.
- The establishment of an Expert & Advisory Board: An external Expert & Advisory Board (EAB) will be established, which will provide valuable inputs at different stages of the project. The

[3] https://guidelines.openaire.eu/en/latest/data/index.html

board will contain experts and will represent a broad variety of actors. Until the start of the PCP the EAB will be opened to further members from the relevant communities. Through this board the consortium will be able to access relevant expertise at certain stages of the PCP and build up direct linkages for further networking and dissemination activities. The board will also contain partners from the previous iProcureSecurity CSA project.

- The establishment of an Observer Board: Procurers beyond the project consortium and who have already shown interest in iProcureSecurity PCP are kept informed of the progress and may wish to also take action by subscribing to the approach of the PCP, becoming an interested observer and staying informed about the solutions being developed throughout the PCP phases.
- The organisation of and the participation in workshops and events of a European iProcureSecurity PCP Symposium for all the relevant stakeholders where the project outcomes will be presented, and ideas will be shared. This will support the engagement of the boards and the project implementation.
- The establishment and creation of the EMS Network, that aims to facilitate the engagement, communication and exchange of information between the suppliers and the procurers. The platform will also serve as hub to present innovative technical solutions in the field of triage management system.

2.2.4 Making data interoperable

The concept of interoperability demands that both data and metadata must be machine-readable and that a consistent terminology is used. The iProcureSecurity PCP partners will observe OpenAIRE guidelines for online interoperability. These guidelines can be found at: https://guidelines.openaire.eu/en/latest/. Partners will also ensure that iProcureSecurity PCP data observes FAIR data principles under H2020 open-access policy: https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-dissemination_en.htm ; https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-pilot-guide_en.pdf

By depositing the project datasets in a data repository compliant with the appropriate interoperability guidelines (OpenAIRE's ZENODO) and by providing a sufficient metadata description of such datasets as mentioned above, iProcureSecurity PCP will ensure that the research data produced in the course of the project activity meet the required interoperability standards. It is also worth mentioning, that metadata vocabularies, standards and methodologies will be adjusted, as commented previously in the current chapter, in order to promote interoperability.

2.2.5 Increase data re-use

Data re-usability is becoming a distinct characteristic of modern scientific practice. By data re-usability, it is meant the ease of using data for legitimate scientific research by one or more communities of research (consumer communities) that is produced by other communities of research (producer communities). Data re-usability allows the reanalysis of evidence, reproduction and verification of results, minimizing duplication of effort, and building on the work of others. It has four main dimensions: policy, legal, economic and technological.

2.2.6 Allocation of Resources

The costs of making data FAIR have been allocated and covered by the iProcureSecurity PCP project budget. Thus, it is foreseen at this point that no extra-costs will be incurred. The dissemination material (e.g. scientific publications) will be made available through OpenAIRE with no additional costs.

2.3 Data Security

No EUCI is handled as part of the iProcureSecurity PCP project.

However, since the security of the data generated or used during the lifetime of the project is prioritized, iProcureSecurity PCP will use state-of-the-art technologies for secure storage, delivery and access of information, as well as managing the rights of the users for the data generated or collected in the project. In this way, there is guarantee that the accessed, delivered, stored and transmitted content is managed by authorised persons.

Security measures, adopted by the iProcureSecurity PCP Consortium, are a set of technological, procedural and organizational requirements aimed at implementing an adequate level of security in data processing, in order to guarantee the confidentiality, integrity and availability of data and the resilience of the systems (analog and digital).

The identification of the appropriate security measures is the result according to a path of analysis, assessment and risk management made by each responsible partner.

Some of the technical measures aimed at guaranteeing the confidentiality, integrity and availability of data and the resilience of the systems are described below:

1. Security tools for paper documents and archives:

    a. Paper document filing systems (cabinets, filing cabinets equipped with locks);

    b. the documents will be kept in an office's secure environment ensuring access only to authorised personnel;

    c. Paper document destruction system;

2. Security tools applied to data:

    a. Management of assignment and management of access privileges and credentials with enabling and disabling of accounts;

    b. Management of all workstations that are connected to the company network;

    c. Logical access control and traceability systems;

    d. Application log management;

    e. Encryption of data in company databases;

    f. Pseudonymisation for some types of data and applications;

    g. Systems for the destruction of digital data archives.

3. Security tools applied to systems:

    a. Physical access control systems;

b. Physical security systems (fire prevention - anti-flooding);

c. Perimeter logical security measures through firewalls and DMZs;

d. Spyware virus protection measures etc.;

e. Use of secure network protocols for accessing applications;

f. Use of network protocols and secure applications for data transmission;

g. Access to software systems exclusively via an internal network;

h. Backup and replacement of data storage;

i. Business Continuity and Disaster Recovery;

j. Systems updating and patching (with respect to the application);

Extended and detailed reference to the security measures for the protection of personal data will be provided by each consortium partner separately and delivered as part of D10.2 POPD-Requirement No.2.

2.4 iProcureSecurity PCP DMP Process and Responsibilities

1. The first step is to **evaluate the nature of the data, open or not open,** in accordance with this DMP principles and the accessibility level for open data sets. **Personal data will not be open. They will be included only in confidential deliverables, if needed. Only anonymized data will be included in public deliverables or open datasets.** For data sets not included in this document the DPM responsible (KEMEA) and the Project Coordinator (SYNYO) should be consulted.
2. The second step, in case of personal data, is to **evaluate the need to request an informed consent** for data collection. If need, the template of Information Sheet and Informed Consent Form should be adapted to the specific task. **Relevant deliverable where this template can be found is D10.1 H-Requirement No.1.**
3. **The Task Leader (Data Controller) is responsible of the organization of the data collection** in the most convenient way. **However, it is not certain that the Task Leader will be the data controller in all cases. It must be examined *ad hoc* based on each data processing operation. E.g., there might be joint controllership or a controller-processor relationship.**
4. Whether the data is public or not, it should be **preserved, archived and managed in an anonymized way, in the Task Leader server**, in case the Task Leader acts as **Data Controller**.
5. Duly signed **Informed Consent forms, must be kept by the Data Controller for a 5-year period** in order to be available for auditing by any competent authority. The data controller is the Leader of the respective Task.
6. The Task Leader should also upload the data in **the iProcureSecurity PCP internal repository.**
7. **For data aimed open it should be uploaded to ZENODO.**
8. After uploading data in ZENODO, Task Leaders should inform the DMP Responsible (KEMEA) and the Project Coordinator (SYNYO) for their follow-up.
9. iProcureSecurity PCP publish in ZENODO the open data sets, deliverables with a public dissemination level (following the GA), articles and publications.

10. **The DMP responsible (KEMEA) together with the Project Coordinator (SYNYO) will oversee that the process** is compliant with this DMP and the GDPR. KEMEA together with the coordinator will monitor the correct implementation of the DMP and discuss updates and questions concerning the DMP on a monthly basis (e.g. during regular project conference calls or meetings).

3 Ethical Aspects – Personal Data Management

Issues related to ethical aspects and to personal data protection are handled explicitly in WP10 'Ethics Requirements' and the respective deliverables D10.1 (informed consent procedures and incidental findings policy for the project), D10.2 (making available of DPO's contact details, data protection policies, technical, organizational and security measures, anonymisation/pseudonymisation techniques, compliance with the data minimization principle, transfer from/to non-EU countries) and D10.3 (copies of opinions/approvals by ethics committees or competent authorities).

With respect to all data processing activities of the project as they are described below in detail, constant guidance will be provided by the Project Coordinator (SYNYO) that is leading WP10 and the Independent Ethics Advisor appointed for the project as well as by the Data Protection Officer of each partner as listed in D10.2 POPD-Requirement No.2. For partners not having appointed a DPO, a data protection policy exists which will be also included in D10.2 POPD-Requirement No.2.

The project consortium commits to the protection of personal data processed during the lifetime of the research project and will implement the appropriate safeguards in order to be compliant with the GDPR provisions. All partners respect the principle of data minimization (relevant deliverable D10.2). Technical and organizational measures as well as security measures will be implemented by each partner (relevant deliverable D10.2). Anonymisation/pseudonymisation techniques will be also implemented by specific partners (relevant deliverable D10.2).

3.1 Important GDPR provisions

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

According to **Recital 26 GDPR**, the principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. Since GDPR does not apply to anonymous information, it is very important to distinguish between anonymised and pseudonymised data, as for the latter GDPR remains applicable.

According to **Article 4 par.7 GDPR**, 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by

Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

According to **Article 4 par.8 GDPR**, 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

According to **Article 5 par.1-2 GDPR**, the principles relating to the processing of personal data are:

- lawfulness, fairness and transparency;
- purpose limitation;
- data minimisation;
- accuracy;
- storage limitation;
- integrity and confidentiality;
- accountability.

According to **Article 6 par.1 GDPR**, processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

Article 13 GDPR stipulates the information that must be provided by the controller to the data subjects when the personal data is collected by them.

Article 14 GDPR stipulates the information that must be provided by the controller to the data subjects when the personal data is not obtained by them. Paragraph 4 (b) provides for that paragraphs 1 to 3 shall not apply when the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89 par.1 or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.

Article 25 GDPR stipulates the "Data protection by design and by default", including procedures for pseudonymisation and data minimisation.

Article 30 GDPR stipulates a "Record of processing activities", according to which an accurate description of the protection activities shall be kept by the data controller and the data processor and, upon request, made available to supervisory authorities.

Article 32 GDPR stipulates the "Security of processing". This article aims to ensure that the data are kept and processed in a secure manner in order to avoid their unlawful or accidental destruction, loss, alteration, unauthorised disclosure or access. Possible measures to enforce data security include pseudonymisation and encryption as well as regular testing of the implemented technical and organisational measures.

According to **Article 35 par.1 GDPR**, where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

According to **Article 89 GDPR**, processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with GDPR, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner.

3.2 Data processing activities

Personal data will be processed during the lifetime of the project for:

1. Coordination and management purposes (WP1);

2. Research activities that involve participants on a voluntary basis, i.e. questionnaires, interviews, workshops, pilot demonstrations and other testing activities (e.g. as part of WP3, WP6, WP7);

3. Dissemination, communication and exploitation purposes (WP9).

3.2.1 Coordination and Management

In the context of WP1, the Coordinator and the Task Leaders will process personal data of the personnel of the Consortium partners for the purposes of the coordination and management of the project, such as names, email addresses, signatures, voice (during online meetings) and image (if necessary during online meetings).

This processing is necessary for the performance of the iProcureSecurity PCP Consortium Agreement and the iProcureSecurity PCP Grant Agreement (art.6 par.1 (b) GDPR).

The personal information is obtained by the data subjects (researchers).

The storage period is for 5 years after the end of the project according to articles 18.1 and 22.1 of the Grant Agreement for accountability reasons towards the EC. Image/voice will be kept for the time period stipulated in section 6.2.5 of the Consortium Agreement for the drafting of minutes.

The recipients will be only the members of the Consortium for information sharing purposes via the project's online repository. The access to the repository is managed by the Project Coordinator and it is protected by usernames and passwords so that only members who have been granted permission can access it. Any transfer to the non-EU partners of the project will be in accordance with Chapter V of the GDPR.

The data subjects have the rights stipulated by the GDPR (right to request information, right to access, right to rectification, right to erasure, right to restriction, right to data portability, right to lodge a complaint with a supervisory authority) and can exercise them by contacting the DPO of the controller or, in absence of a DPO, by contacting the controller itself.

The contact details of the partners' DPOs are made available in this deliverable and any updates will be made available in D10.2 POPD-Requirement No.2. In absence of a DPO, the contact details of the partners acting as controllers will be made available in the aforementioned deliverable. The organisational, technical and security measures implemented by each partner acting as controller will be presented and described in D10.2 POPD-Requirement No.2.

3.2.2 Research activities that involve personal data obtained by the data subjects (volunteers)

With respect to the procedures which shall be followed for the participants' personal data processing, the researcher carrying out interviews/questionnaires/workshops/pilots with volunteers must inform the participants in advance via a detailed Information Sheet in accordance with art.13 GDPR.

The request for consent will be presented in an intelligible and easily accessible form, using clear and plain language. In case of any questions during the carrying out of a research activity, the researcher will be there ready to respond and make clarifications.

A copy of the Information Sheet will be provided to the research participants, in order for the researcher/data controller to be sure that they will be able to read the information therein at any time and that they will exercise their rights whenever they see the need to do so.

After ensuring that the participant has read and understood the information included in the Information Sheet, the researcher shall provide the participant with an Informed Consent Form for data processing.

The Informed Consent Form shall be signed by the participant if he/she consents to the data processing. The participants can withdraw their consent at any time without consequences.

The personal information on the Informed Consent Form will be processed in compliance with the General Data Protection Regulation and will be stored securely for the time period mentioned in articles 18.1 and 22.1 of the iProcureSecurity PCP Grant Agreement (5 years after the end of the project) for accountability reasons.

Extended reference to the informed consent procedure for data processing will be made in D10.1 H-Requirement No.1. The relevant templates will be provided therein.

3.2.3 Research activities that involve personal data not obtained by the data subjects

It will be examined as part of D10.1 H-Requirement No.1 whether any data processing operations as part of the project's research activities are not based on the consent of the participants/data subjects either because it would impossible to obtain such consent or it would require disproportionate effort. Article 14 GDPR shall be applicable in such cases. All necessary safeguards to be implemented will be presented in D10.2 POPD-Requirement No.2.

3.2.4 Dissemination, communication and exploitation of project's results

The project's website will always function as the primary source of available information. Through it, information will be provided about the consortium, planned work and events. The web portal will promote dissemination and communication activities by featuring press releases, publications and conference presentations. iProcureSecurity PCP will produce electronic newsletters and blogposts, published through the project's web-portal presenting ongoing activities and future planning of the project's activities. Same purpose is served by the project's social media accounts.

During each meeting or event as part of WP9, personal information of the researchers and other participants attending the meeting/event are taken for registration and participation purposes, provided that they have consented to this.

To this end, before the start of each meeting/event, an Information Sheet for data processing will be distributed to the attendees wherein it will be explained with the information indicated in art.13 GDPR.

The organisational, technological and security measures implemented by the controller(s) are explicitly mentioned in D10.2 POPD-Requirement No. 2.

4 Intellectual Property Rights (IPR) Management

All partners in the consortium have agreed on explicit rules that need to be concerned as regards to the IP ownership. In that way, access rights have been given to any Background and Foreground for the execution and protection of intellectual property rights (IPR) and confidential information before the project starts. All details have been addressed within the Consortium Agreement between all project partners.

4.1 Definitions

Intellectual Property Rights or IPR(s) means patents, patent applications and other statutory rights in inventions; copyrights (including without limitation copyrights in Software); registered design rights, applications for registered design rights, unregistered design rights and other statutory rights in designs; and other similar or equivalent forms of statutory protection, wherever in the world arising or available, but excluding rights in Confidential Information and/or trade secrets.

Background means any data, know-how or information — whatever its form or nature (tangible or intangible), including any rights such as intellectual property rights — that:

- is held by the beneficiaries before they acceded to the Consortium Agreement, and
- is needed to implement the action or exploit the results.

Foreground or Result(s) means any tangible or intangible output of the Project, such as data, knowledge and information whatever their form or nature, whether or not they can be protected, which are generated in the Project as well as any rights attached to them, including intellectual property rights.

4.2 IPR Management in the iProcureSecurity PCP Project

The iProcureSecurity PCP consortium Agreement expressly stipulates the rules related to the management of IP rights and distinguishes, on the one hand, the IP rights that are held by the partners prior to their accession in the Consortium Agreement and are needed for the Project (Background) and, on the other hand, the IP rights that are held by the partners during the lifetime of the Project (Results).

In particular, Section 8-Results and Section 9-Access Rights of the iProcureSecurity PCP Consortium Agreement include all relevant clauses that have been agreed between the partners and refer to the IPR management. In Attachment 1 of the Consortium Agreement, the Parties have identified and agreed on the Background for the Project and have also, where relevant, informed each other that access to specific Background is subject to legal restrictions or limits. Therefore, we aim to work methodically in order to classify iProcureSecurity PCP IPRs and define:

- the treatment of existing IPRs (background),
- the management of joint ownership. Partners will keep record of their contributions which are protected by IP Law and potentially Trade Secrets. This will permit the consortium to discern the share of each owner in relation to the results of a joint effort. The consortium partners aim to reach a point where exploitation of results will become possible.
- the protection and management of the project's results (foreground),
- the exploitation and dissemination of the project's results (foreground),
- the protection of know how created during the project.

Furthermore, section 4 and section 5 of the iProcureSecurity PCP Consortium Agreement provide for the responsibilities of the partners and their liability towards each other (including for the management of IP rights).

All partners may settle any disputes in accordance with the clause 11.8 of the Consortium Agreement.

5 Open Access to Scientific Publications

Each beneficiary must ensure open access to all peer-reviewed scientific publications relating to its results. Open access to scientific publications refers to free of charge online access for any user. Open access will be achieved through the following steps:

1. Any paper presenting the project's results will acknowledge the action: "The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101022061 - iProcureSecurity PCP" and display the EU emblem.
2. Any paper presenting the Action results will be deposited at least by the time of publication to a formal repository for scientific papers. If the organisation does not support a formal

repository (https://www.openaire.eu), the paper can be uploaded in the European sponsored repository for scientific papers: http://zenodo.org/

3. Authors can choose to pay "author processing charges" to ensure open access publishing, but still they have to deposit the paper in a formal repository for scientific papers (step 2).
4. Authors will ensure open access via the repository to the bibliographic metadata identifying the deposited publication. More specifically, the following will be included:
    a. The terms "European Union (EU)" and "Horizon 2020";
    b. "iProcureSecurity PCP - Pre-Commercial Procurement of Innovative Triage Management Systems Strengthening Resilience and Interoperability of Emergency Medical Services", Grant agreement number 101022061;
    a. Publication data, length of embargo period if applicable; and
    b. A persistent identifier.
5. Each case will be examined separately in order to decide on self-archiving or paying for open access publishing.

6 Open Access to Research data

Open access to research data refers to the right to access and re-use digital research data generated by Actions. As per GA 101022061 iProcureSecurity PCP section 29.3, Open Access to Research Data is applicable in iProcureSecurity PCP (see section 2.2.1 above).

7 Conclusion

The present deliverable constitutes the Data Management Plan as it has been formed in Month 5 of the iProcureSecurity PCP project. The DMP is a living document that evolves during the lifetime of the research. Since this is an early stage, a second version (D1.5) is foreseen to be added as a deliverable in Month 12 of the project in order to give a clearer and complete overview of the generated and used data and cover any gaps that exist in the present. A final updated version will follow in Month 36 (D1.6).

This deliverable must be intended as a useful guide with respect to data management, reporting the main principles that the iProcureSecurity PCP project is adherent to and providing a snapshot on the security and ethics/privacy related aspects.

References

Data Management, (2020),https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm

Consortium Agreement for the iProcureSecurity PCP project

Grant Agreement No 101022061 for the iProcureSecurity PCP project

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

Annex I

All partners commit to continuously keep track of the specific data sets processed under the tasks they are leading and to report them internally by completing the following table:

[PARTNER INITIALS], WP[No.], T[No.] *(e.g. TLX, WP1, T1.2)*	
Data set	*Name of the data set and reference*
Description	*Description, source of the data, creation method,…*
File format	*Software or file format used to work with the data – e.g. Word,…*
Metadata	*Data characteristics*
Data sharing	*Data derives from…, is shared with…, is used by…*
Archiving and preservation	*Data are stored… Backups,…*
Additional information	*Are you generating the data or sourcing it from elsewhere? Are there certain terms and conditions applicable?* *Is the data digital or non-digital? Both?* *How will the data be created or collected? What instruments or tools will be used?* *What transformations will the data undergo?* *Will the data be updated or become redundant as you make revisions and produce subsequent versions?* *Are you processing information that falls outside of the scope of this DMP? E.g. confidential information.*