Ref. Ares(2020)6113760 - 29/10/2020

HORIZON 2020

D1.5 DATA MANAGEMENT PLAN

Augmented Reality Enriched Situation awareness for Border security
ARESIBO – GA 833805

Deliverable Information

Deliverable Number: D1.5
Work Package: 1
Date of Issue: 31/10/2020
Document Reference: N/A
Version Number: 0.5
Nature of Deliverable: Report
Dissemination Level of Deliverable: PU (PU / RE / CO)
Author(s): CBRA
Keywords: data governance, data protection, security policies, FAIR principles

Abstract:

D1.5 Data Management Plan describes the data management life cycle for all data sets that will be collected, processed or generated by the project. It outlines how research data will be handled, 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 document details ARESIBO data governance, with responsibilities of the Data Protection Officer (DPO), Project Security Officer (PSO) and Ethical Manager. Data protection and security policies followed by the project are also presented. This is version 1 of the Data Management Plan, which will be updated in version 2 due at the end of the project.

Document History

Date	Version	Remarks
15.02.2020	0.1	**Very preliminary draft based on information from project document and partners' info for other tasks and WPs**
17.04.2020	0.2	**Second version with inputs of the ARESIBO Project PSO**
06.05.2020	0.3	**Third version with additional inputs from ADS**
26.06.2020	0.4	**Fourth version with inputs from partners**
08.09.2020	0.5	**Fifth version with additional inputs and revisions**
30.09.2020	**0.6**	**Final draft sent for quality review**

Document Authors

Entity	Contributors
CBRA	**Vittoria, Luda di Cortemiglia Toni, Mannistö;Vladen, Tsikolenko**
BDI	**Nikolai, Stoianov; Ilian, Hutov and Pavlina, Nikolova**
MARINHA	**Vítor Fernando, Plácido da Conceição**
ISIG	**Olivia, Ferrari and Marina, Andeva**
CMRE	**Alberto, Tremori; Luca, Berretta**
HMOD	**Andreas, Tsigiros**

Disclosure Statement:

The information contained in this document is the property of ARESIBO Consortium and it shall not be reproduced, disclosed, modified or communicated to any third parties without the prior written consent of the abovementioned entities.

Table of Contents

List of Acronyms

Acronym	Meaning
AR	Augmented Reality
DOA	Description of Action
DPM	Data Management Plan
DPO	Data Protection Officer
EDA PADR	European Defence Agency Pilot Project and Preparatory Action on Defence Research
ERC	European Research Council
EUCI	EU-Classified Information
EU	European Union
EUROSUR	European Border Surveillance System
FAIR	Findable, accessible, interoperable and reusable
FSC	Facility Security Clearance
GDPR	General Data Protection Regulation
IMO	Impact-making Objective
NISO	National Information Standards Organization
OP	Open Access
ORDP	Open Research Data Pilot
ParDPO	Partner Data Protection Officer
PMB	Project Management Board
ParPSO	Partner Project Security Officer
PSC	Personal Security Clearance
PSO	Project Security Officer
RIO	Research and Innovation Objective
SAB	Security Advisory Board
WP	Work package

Executive summary

This document is the first version of deliverable D1.5 Data Management Plan v.1 of the European project “Augmented Reality Enriched Situation awareness for Border security-ARESIBO” (GA 833805). The updated final version of this deliverable will be submitted at the end of the project in M 36.

The Data Management Plan (DPM) describes the types of data that will be produced, collected and/or processed during the project and how this data will be handled after the project. The objective of the data management plans is that all types of data useful to the project (and other projects as well) are clearly identified, FAIR (easily Findable, openly Accessible, Interoperable and Re-usable), that they don’t raise any ethical or security concern.

This document has been prepared by taking into account the template of the “Guidelines on Data Management in Horizon 2020” [version 3.0 of 26 July 2016]. The elaboration of this Data Management Plan will allow ARESIBO partners to address all issues related with data protection, including ethical and security Protection concerns.

The DMP is intended to be a living document. At this stage a number of questions related to the data are still open for discussion. In particular, questions related to how to make data findable, accessible, interoperable and reusable (FAIR) will have a provisional answer in this deliverable, which will be updated once all the necessary levels of information will be obtain over the next months. Also, at this point in time (M18), very little pseudo-anonymised data has been collected and stored in the password-protected cloud environment of the project (https://procloud.di.uoa.gr/). Data requiring security clearance are stored in the respective platform by individual partners collecting them and storing them in accordance their agency/institutional requirements.

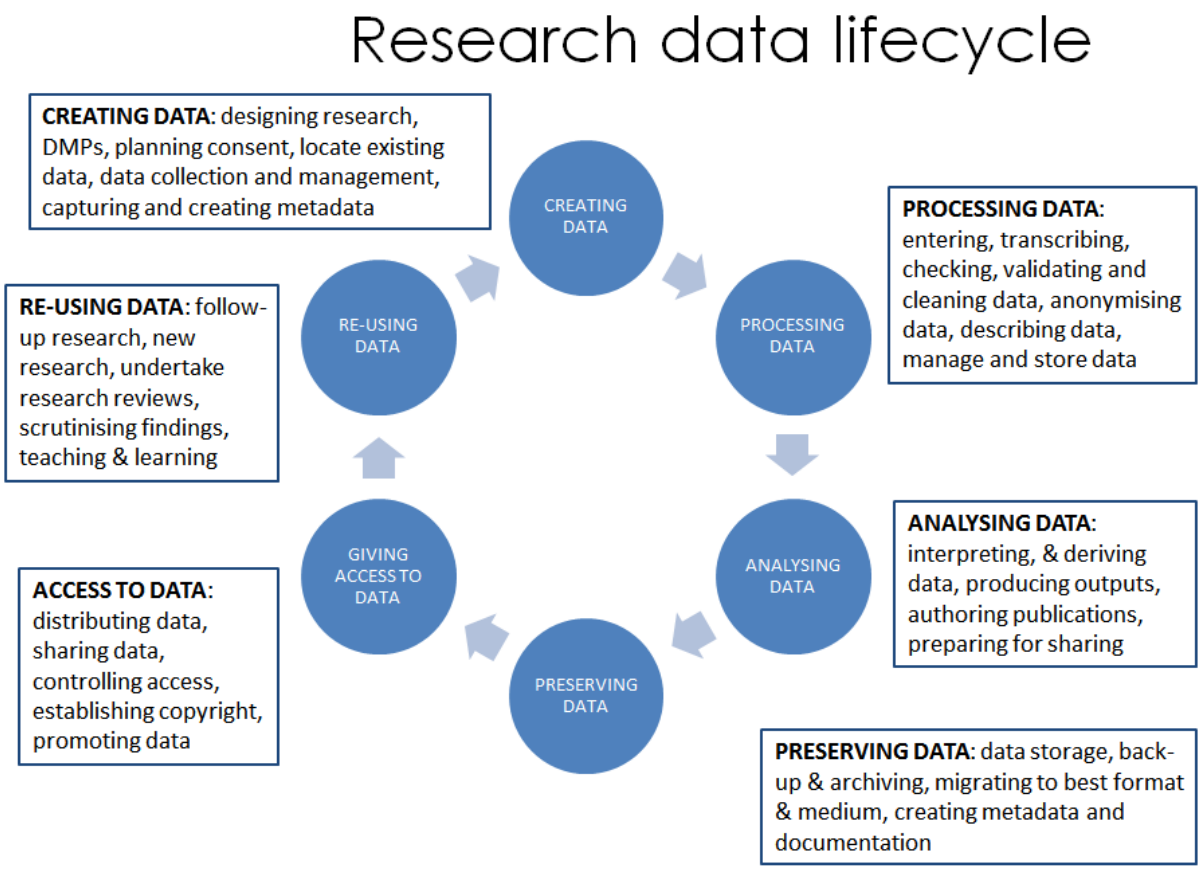
1 Introduction

Data management enables knowledge discovery and supports innovation, by data and knowledge integration and reuse. Project Data Management Plans (DMPs) are a key element of good data management in every EU project.

Research in ARESIBO deals with border security issues and critical information which may raise security concerns. A major priority for the partnership is thus to secure the material collected or produced by partners in this research. Therefore, data security policies applied within ARESIBO will be detailed in the DPM. In parallel, as Horizon 2020 has the aim to accelerate research by making data findable, accessible, interoperable and reusable (FAIR), it also requires effective data management. Data management, in fact, enables knowledge discovery and supports innovation, by data and knowledge integration and reuse. Project Data Management Plans (DMPs) are a key element of good data management in every EU project.

The main goal of the Data Management Plan (DMP) is to specify the data management life cycle for all data that will be collected, processed or generated by the project. It will provide an outline of the data types the project will generate, whether and how it will be exploited or made accessible for verification and re-use, and how it will be curated and preserved. This task will support the continuous identification, monitoring, qualification and use of data produced by participants and used in the ARESIBO project, and the data security policies to be followed along the entire process.

The data cycle is the following one (EUDAT – OpenAIRE):[1]



[1] See https://www.openaire.eu/search?q=EUDAT&option=com_finder&Itemid=1860

At each step of the cycle, the IPRs and contractual clauses need to be respected. In particular: who owns these data, is the process applied to these data allowed, where will the data be stored and during how much time, who can have access to these data, to do what?

In addition, according to the "Guidelines on Data Management in Horizon 2020", the DMP will also have the aim to produce data that other researchers may benefit from. For these reasons, data generated by research in Horizon 2020 projects that are:

- Discoverable;
- Accessible;
- Interoperable to specific quality standards; and
- to create data sets enabling reproducible and verifiable research results by others.

In general terms, the ARESIBO DMP requirements are defined within the context of the Grant Agreement (GA). Data Management Plan is an internal document, designed to evolve through the ARESIBO project lifespan, capable to capture and reflect evolution in the form of dataset updates and/or changes in Consortium policies. Two versions of the DMP are expected: the first and present one in M18 (October 2020), and the second in M 36 (April 2022).

The most important explanations for setting up the ARESIBO DMP are:

- To ensure full respect and observance of security and ethical issues throughout the implementation of the project.
- To embed the ARESIBO project in the EU policy on data management which is increasingly geared towards providing open access to data that is gathered with funds from the EU.
- To comply with the Horizon 2020 Open Data Access Guidelines.
- To enable the verification of the research results and the sustainable storage of data in the ARESIBO platform.

Therefore, the AREISBO DMP provides a description of the data management life cycle for the data collected, processed, generated. In particular, the ARESIBO DMP considers:

- the data generated, collected, processed mainly coming from sensors, videos, audios and other ARESIBO solutions, but also through interviews and questionnaire to end users and stakeholders;
- the method to applied in the data life-cycle and the related standards, as addressed in WP1 – Task 1.4 and 1.5;
- the definition of the data sets that are shared/made open access; and
- the methods used for data management and preservation after the end of the project.

The consortium, as detailed further under 2.2.2.5, will decide which data are part of an open data scheme, and therefore available for the Open Access Data initiative. Various mechanisms to protect identities and sensitive information have been foreseen and will be carefully implemented throughout the projects, as a part of the data management actions.

In any case, ARESIBO will not publish any confidential data and results under Open Access through the scientific publications produced along the project lifecycle.

2 ARESIBO Data Management Plan

ARESIBO partners have drafted the DMP in full compliance with the legal and ethical requirements identified in T1.4 and in WP9 Ethics. The structure of the DMP follows the Horizon 2020 Guidelines.

2.1 Data Summary

This section aims to provide a review of the scope of the project (purpose and objectives) in order to clarify the relation between it and the data generation, collection and processing envisaged by the project. A more in-depth description of the data summary of each WP is provide in Annex B.

2.1.1 The purpose and objectives of ARESIBO

ARESIBO aims to create and test a new system based on technologies to enhance situation awareness and implement an integrated Augmented Reality (AR) capability around a private "cloud" for both tactical C2 centres and field units involved in border surveillance and control (with two sub-models: one for the land borders and one for the maritime borders).

Below the Research and Innovation Objectives (RIOs) of ARESIBO, as presented in the Description of Action (DoA), will be shortly summarised, indicating relevant data sources.

RIO-1: Integrated situation awareness and improved perception for field and C2 operators through intuitive AR interfaces
The complexity of border security operations calls for enriched user interaction that can increase the perception capability of the operators and time efficiency in the accomplishment of tasks. ARESIBO will develop and test a wide range of sophisticated AR functionalities and tools for both to the field and Command and Control Center operators, based on information provided through an interoperable data interface.

RIO-2: Better human-robot collaboration via dynamic UxV swarm intelligence for optimised surveillance
Collaboration and exchange of data between unmanned vehicles and field units is essential for operational activities. Data from sensors, cameras, microphones, etc. will be collected and exchanged, to improve surveillance missions.

RIO-3: Secure the network connectivity between the field units and the C2 via Intelligent Hybrid Networks and Edge Computing

The ARESIBO communication solution will allow cooperation and exchange of data between field units and between field units (including both land and maritime operations) and C2. Data from sensors, UxV and humans will be exchanged through the connection with the cloud infrastructure. Edge computing techniques will be employed.

RIO- 4: Help operational units familiarize with the new IT tools by means of Serious Games

ARESIBO envisages the development of an integrated training environment by means of Serious Games, to facilitate the learning process of operators. Relevant data and information

will stem from the data collection carried out for the development of the technological WPs, and in particular within WP4 and WP5.

RIO- 5: Cross-platform interoperability of data-, user-, and network- interfaces and contribution to standards
ARESIBO will adopt standards by NATO (e.g. STANAG 4586 for UAVs, JASUS/JANUS for UxV, etc.) to ensure interoperability of existing legacy systems and regional/national information sources. Data will stem from distinct UxV platforms and payload/sensors.

RIO 6: Holistic decision making based on Situational Awareness Assessment and Forecasting Tools
ARESIBO will develop a holistic decision-making support tool, equipped with: 1) situational awareness capabilities; 2) situational assessment capabilities; and 3) situational forecasting capabilities. The information that will be automatically generated by the decision support tool will be presented to the operator. Data will stem from a variety of sources including, among the visual recognition of objects based on Deep Learning Technology, sensor streams, radar information, but also document and reports, and risk analysis documents.

In addition, in ARESIBO foresees the six Impact Making Objectives (IMOs). Below a short description of the data and information which will be useful to reach them:

IMO-1: Dissemination and collaboration
ARESIBO will disseminate the project results, especially with border control authorities, LEAs and the security and defence community and establish synergies with other projects working in the same domain. Methods for data sharing and contribution to the Open Research Data Pilot will be described in detail below under paragraph 2.2.5.2

Several ARESIBO partners participate in the European Defence Agency Pilot Project and Preparatory Action on Defence Research (EDA PADR)[2] projects. ARESIBO will provide orientations to enhance the European Border Surveillance System (EUROSUR)[3] handbook and the legislative document by providing return of experience from the tests and demos performed in real and realistic environments in WP 7 (Live trials and testing) with the support of the end-users. ARESIBO platform will be tested and demonstrated in three different types of environment, land-borders, sea-borders, and mixed environments in four different countries (FI, GR, BG, PT). In addition, relevant data will also be shared with the project External Advisory Board (EAB) composed of knowledgeable practitioners and experts in border security.

IMO-2: Exploitation and sustainability model
ARESIBO aims to foster market growth of interoperable system-of-systems to establish a core EU expertise in the integration of Augmented Reality systems in border security operations. Data and information on the potential impact of such technologies and for the development of a market analysis will be collected by end users and other stakeholders by means of questionnaires and dedicated workshops.

IMO-3: Increased perception of security by EU citizens
ARESIBO will assess the potential impact of the developed solutions and technologies on societal level. The active participation of citizens will be pursued through dedicated workshops and dissemination questionnaires for the collection of the relevant information.

[2] See https://www.eda.europa.eu/what-we-do/activities/activities-search/pilot-project-and-preparatory-action-for-defence-research
[3] See https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/border-crossing/eurosur_en

IMO-4: Ensuring that the technologies developed within ARESIBO are accepted by citizens and are compliant with the current legal framework
Similarly, to IMO-3, the consortium will develop ARESIBO solutions taking into account citizens' perceptions and acceptance of security measures. Necessary information will be acquired through a questionnaire will be targeting citizens from EU external border crossings such as airports and land border crossings between non-EU states and EU MS participating in the project.

IMO-5: Effective cross-border cooperation and management by stimulating cross-border dialogue
End-users' personnel will be actively involved in order to ensure harmonisation of operational requirements. Dedicated questionnaires have been disseminated to collection end users requirements; the information collected was also extensively discussed during dedicated end-users workshops and teleconference meetings.

2.1.2 Type and format of data generated and used by ARESIBO

As outlined in the DoA, different type of data generated and used within ARESIBO will stem from different data sources throughout the execution of the project. This data mainly consists of:

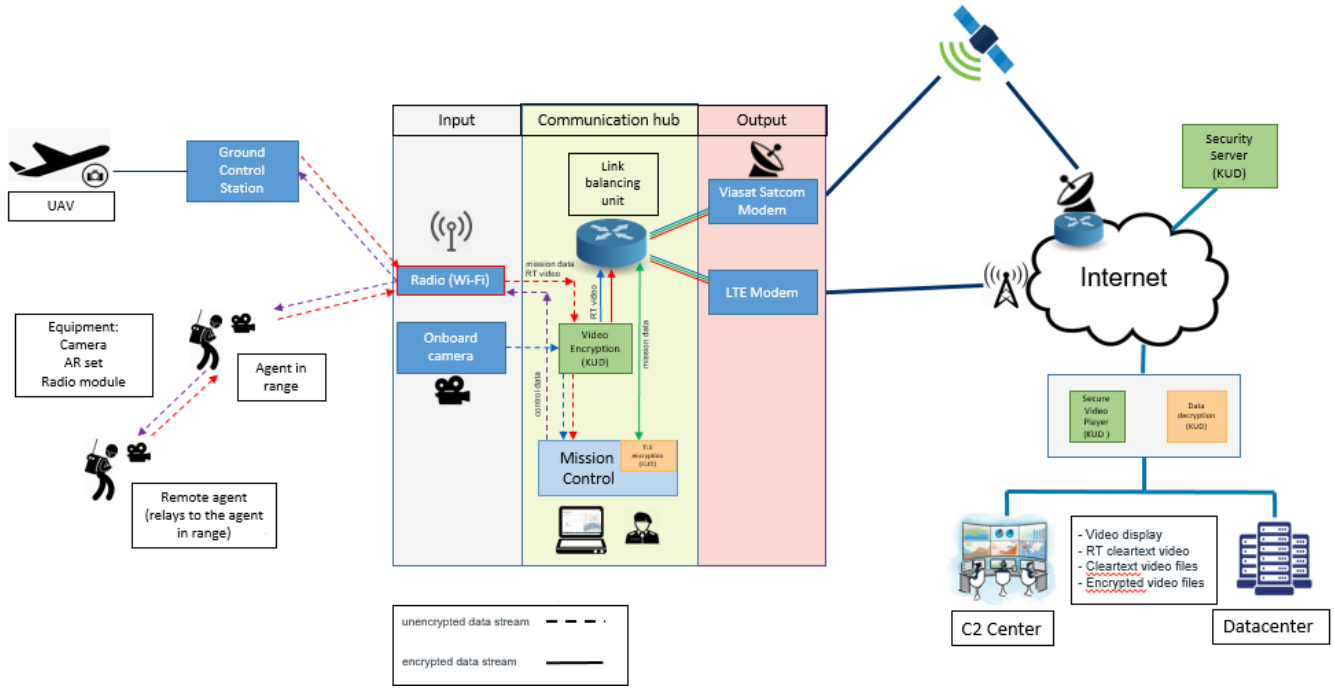
- Documents/Reports
- Images
- Maps
- Videos (drone, external cameras, etc.)
- Other sensors (e.g. motion sensors)
- Audio (e.g. voice stream)
- Geographic coordinates
- Telemetry Data
- Radar information
- Interviews/Questionnaires.

The sources of data generated and or used within ARESIBO include:

- cameras
- microphones
- real-time sensors, acoustic sensors and visual sensors including RGB, IR, thermal cameras
- radar
- satellite
- software system data (aggregated data, analyzed data, clustered data …)
- open sources.

A more detailed explanation of different data types, format and sources across the nine ARESIBO Work Packages is provided in Annex B.

Fig. 1 ARESIBO data sources



These data will be originated/provided by partners (both end users and research partners) either by using the ARESIBO solutions and partners' hardware (AR devices, sensors, UxVs, etc.), or through research activities (such as questionnaires, workshops and interviews).

Size of data varies from a few bytes (e.g., a sensor value) to several Mb such as multimedia presentations or video tutorials. The format of the data will vary from plain text files to PowerPoint presentations, Excel sheets, Docx documents and PDF files. The format of the data will be based on JavaScript Object Notation (JSON)[4] (except for videos).

As regards ARESIBO data utility, the data generated and collected by the project will be useful primarily to project partners involved in the development and test of the ARESIBO solutions and system, but also for end users and stakeholders involved in border security outside the consortium will be able to benefit from some of the data that will be made freely available through dissemination activities. In particular, as mentioned, WP8 deals with dissemination activities aimed at different target groups, such as:

- Border control authorities;
- Law enforcement agencies (LEAs);
- Practitioners;
- Technology and domain experts;
- Scientific community (incl. R&D);
- Border security industry;
- National/international governmental and regulatory bodies;
- General public.

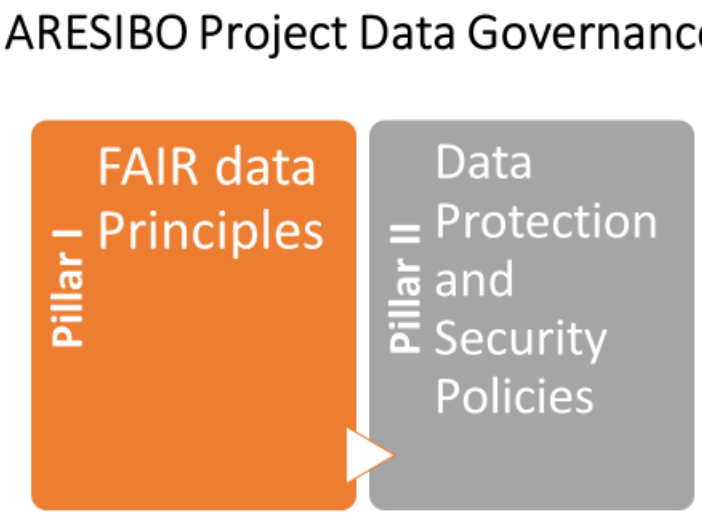
Other projects and initiatives in the field will also benefit from the data collected by ARESIBO, such as EDA PADR and EUROSUR.

[4] JSON is a lightweight data-interchange text format that is completely language independent but uses conventions that are familiar to programmers of the C-family of languages (eg. C, C++, C#, Java, JavaScript, Perl, Python, and many others). See https://www.json.org/json-en.html

2.2 Data Governance

Data governance deals with data usage, consumption and policies. ARESIBO data governance is based upon two main pillars: FAIR data principles, and Data Protection and Security Policies.

Fig. 2 ARESIBO Data Governance Pillars



Complying to the H2020 overall strategy for research, ARESIBO data governance will follow as much as possible the FAIR data principles, whereby all research data should be Findable, Accessible, Interoperable and Reusable (FAIR). This means that data are:

- identified in a persistent manner using the metadata conventions described below under 2.2.4;
- stored in such a way that they can be accessed (with different access levels);
- structured in such a way that they can be combined with other data sets;
- licensed or have terms-of-use that define how they can be used.

ARESIBO data governance classifies data sets based on their usage in ARESIBO and relevant security issues entailed, defining the necessary policies around the usage and consumption of such assets (see in particular section 2.2.5 and 2.2.6 below).

In addition, ARESIBO data governance pays great attention to the data quality as ARESIBO is highly dependent on different type of data from different sources. Hence, priority governance concerns are the data quality ensured throughout the data life cycle and the data security. Security issues are also extremely relevant in the context of ARESIBO and will be dealt in detail in section 2.3 below.

The project aims to assure the very highest quality in all the information and analysis it provides. ARESIBO has established quality control process (see Deliverable 1.1), whose underlying principles are: document procedures, standards and control, issue control for documents, reporting procedures, frequency and format, communication procedures, corrective actions, exception control, conflict resolution, meeting draft agenda, format of meeting minutes, tracking system for actions, specific responsibilities within the project. Fraunhofer IML leads the quality assurance activities in ARESIBO. With regards to Project

Deliverables: each project deliverable is assigned to one leading responsible partner, which takes the responsibility that the deliverable is of high quality and timely delivered. In addition, internal quality reviewers (minimum 2) assess each deliverable and provide inputs and comments to the Quality Assurance Team which are consolidated before the final submission. The present document has undergone this process.

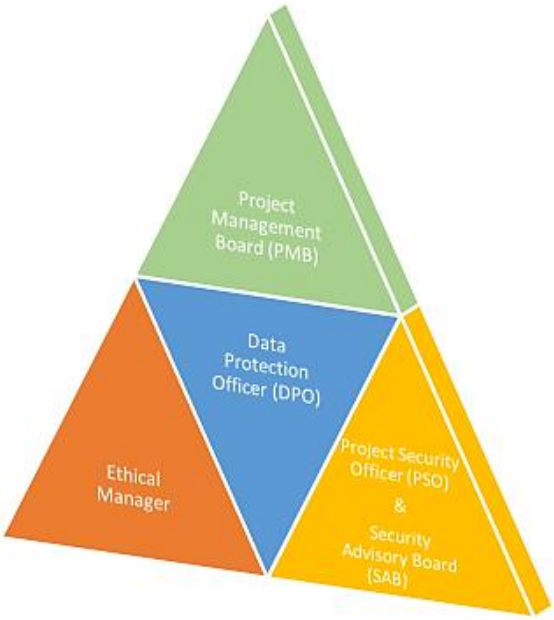
Data governance in ARESIBO ensures the proper data management of important and sensitive data including information coming from sensors and hardware components of the ARESIBO solutions, to be appropriately managed, anonymized, encrypted and sanitized, managing risks which should arise upon their access by third parties.

This data governance strategy is intended to help ARESIBO partners to make the best value of all data collected and/or used with the ARESIBO solutions, to leverage opportunities coming from prediction, risks management and sharing, collaboration and innovations in business models.

The data governance in ARESIBO is exercised and monitored at different levels: central level as well as partners' level. At central level, the ARESIBO Data Protection Officer (DPO) will be responsible for data protection aspects and will liaise with the ARESIBO Project Security Officer (PSO), and the Security Advisory Board (SAB) (see below point 2.3.2). The DPO will also consult with the Ethical Manager, where appropriate. Roles and responsibilities of each actor is summarised below (See also Fig.4).

The ARESIBO DPO periodically reports to the Project Management Board (PMB). All partners are represented in the PMB and therefore have full control of how ARESIBO data are managed, accessed, stored, and - wherever possible - disseminated via the Open Data Access Initiative (see paragraph 2.2.5 below).

Fig. 3 ARESIBO Data Governance Actors (central level)



At a lower level, upon request of the DPO, each partner of the consortium has nominated the respective Partner Data Protection Officer (ParDPO) (detailed in ANNEX A[5]). Partners having the required security clearance have also nominated a Partner Project Security Officer (ParPSOs) (see ANNEX A).

2.2.1 Responsibilities of the ARESIBO DPO

The main responsibilities of the ARESIBO DPO are as follows:

1. Ensures that the DMP clearly outlines data protection procedures to be followed by all partners over the course of the project;
2. Liaises with ParDPOs and ParPSOs for the implementation of the outlined procedures;
3. Consults and liaises with the PSO and the SAB for specific issues related to security aspects;
4. Consults and liaises with the Ethical Manager for specific issues concerning ethics;
5. Periodically reports to the PMB.

2.2.2 Responsibilities of the ARESIBO PSO

The main responsibilities of the ARESIBO Project PSO are as follows:

1. Ensures that the DMP specifies security procedures for all data generated and used within ARESIBO.
2. Ensures that the DMP clearly outlines security procedures to be followed for protection of EUCI in accordance with the EU Council Decision on the security rules for protecting EU classified information (2013/488/EU) and EC Decision on the security rules for protecting EU classified information (2015/444).
3. Ensures that the SAB is established with participation of between five (5) and ten (10) of the project partners. The SAB will be responsible primarily for the review of project deliverables and assessing if they include or may include classified information and, if so, assigns the level of classification and the technical security measures necessary to protect the classified information. The PSO and SAB members have at minimum a security clearance at level of EU Confidential. The SAB is composed of security experts and representatives of end-users with a strong background of handling sensitive information. The beneficiaries concerned have committed not to utilise the EUCI information provided or generated, other than for the specific purpose of the grant agreement. The PSO is supported by the SAB.

2.2.3 Responsibilities of the ARESIBO Ethical Manager

The main responsibilities of the Ethical Manager are defined in the ARESIBO Grant Agreement, specifically under section 3.2.1.7. The Ethical Manager ensures that there is a throughout protection of individuals from all forms of discrimination. In addition, as envisaged by Section 5.1 Ethics (sub-section 5.1.1 Protection of personal data), the Ethical Manager collaborates with the Project Manager in matters related to personal data protection regulated under the EU General Data Protection Regulation (GDPR).

The main task of the Ethical Manager is to define the ethical and societal framework of the project. This task will be performed through:

1. Defining of rules for the project in compliance with research ethics European and international guidelines.

[5] ANNEX A is available for internal distribution only. In the public version of this deliverable ANNEX A names are omitted.

2. Offering support when independent audit is performed in the field of ethics and verify the implementation of ethical requirements in the project
3. Giving assessments on ethical issues in several (strictly defined) ethical and societal project reports / deliverables.
4. Monitoring research activities in the field of ethics as well as ethics concerns in the project.
5. Cooperating with project partners and assisting/facilitating the full respect of project ethical requirements.
6. Ensuring that the project respects protection of all forms of discrimination based on gender, age, race, ethnicity, religion, belief, disability and sexual orientation during the project activities, especially during: a) interviews with citizens; and b) trials specifications and demonstration activities.
7. Supervising WP9 (Ethics), collaborating with the ARESIBO Project Manager in the implementation of WP9 activities.

Fig.4 Roles and responsibilities of DPO, PSO and Ethical Manager

2.2.4 Metadata classification within ARESIBO

For every data collected and/or processed within ARESIBO to be in line with the FAIR principles, it needs to include a reference and name; a description and follow specific standards for metadata. Descriptions of the data that is generated or collected will have to detail its origin (in case it is collected), nature and scale and to whom it could be useful, and whether it underpins a scientific publication. Information on the existence (or not) of similar data and the possibilities for integration and reuse. The data resources' description will be classified using metadata grounded by several standards.

Metadata should be structured in a way that allows describing, explaining, and locating data, in order to make it easy to retrieve, use, or manage the information resource. Metadata can describe resources at any level of aggregation. It can describe a collection, a single resource, or a component part of a larger resource. For the National Information Standards Organization (NISO) there are three types of metadata (NISO, 2004):

- *Descriptive metadata* is used for discovery and identification, as information to search and locate a resource (e.g. for an object/data, the name/designation, the author/source, purpose/subject, characteristics/keywords, supplier/publisher);
- *Structural metadata* describes the components' arrangement of the resource (e.g. for an object/document how parts/pages are organized to form the components/chapters).
- *Administrative metadata* refers to the technical information (e.g. for an object/data the creation time, location and by whom, as well as its type). Two sub-types of administrative metadata are:
    - *Rights management metadata* addresses the intellectual property rights
    - *Preservation metadata* contains information to preserve and save a resource.

Metadata can be achieved through a metamodeling process, a technique used in software engineering and systems engineering for analysis and construction of metamodels (OMG, 2017). Metamodeling is intended for the analysis, construction and development of metamodels (e.g. a kind of UML class diagram) of a certain class of problems using basic structures such as entities, relationships, and constraints, as well as notions such as generalization, association, multiplicity and aggregation. On the other hand, since metadata reflect the knowledge about the systems from which they were derived, an ontology can be used for the elicitation of the properties of a subject area and how they are related among themselves. So, the ontology allows for the definition of the set of concepts and categories that represent the subject. More formally, the ontology encompasses the representation, naming and definition of the categories, properties and relations between the concepts, data and entities that substantiate a certain domain of discourse. In this context the Web Ontology Language (W3C, 2012), as a family of knowledge representation languages, can be used for authoring a specific ontology. A number of tools are available for building metadata (SU, 2019).

The main metadata standard used within ARESIBO will be the Dublin Core Metadata Element Set (DCMI, 1995), which prescribes a set of fifteen generic elements, for resources description: *Creator*, *Contributor*, *Publisher*, *Title*, *Date*, *Language*, *Format*, *Subject*, *Description*, *Identifier*, *Relation*, *Source*, *Type*, *Coverage*, and *Rights*.

These elements are supplemented by a list of qualifiers approved by the Dublin Core Usage Committee (DCMI, 2000). For instance, the *Type* element is a descriptor for the nature, genre and physical manifestation of a resource (e.g. image, video, sound, text, etc.), of predefined type (DCMI, 2020) in a specific format (IANA, 2020). On the other hand, the *Creator* element, allows referencing the originator of a data resource (e. g. person, organization, or service such as UAV, radar, software, IoT device, satellite, etc.).

Several other standards, related with specific datasets, will be assessed for data description of data generated in ARESIBO, namely:

- The ISO/IEC 11179, which targets the representation of metadata for an organization in a metadata registry (ISO, 2019). The ISO/IEC 11179 documents the standardization and registration of metadata to make data understandable and shareable.
- The Data management and interchange subcommittee of ISO-IEC JTC1 is also developing standards for the specification and management of metadata and has issued a technical report on Procedures for achieving metadata registry content consistency (ISO, 2003).
- The ISO Technical Committee 211 (ISO TC 211) developed metadata standards for applications in geographic information systems (ISO, 2003a). Some corporations, such as Microsoft (Microsoft, 2018), also made contributions for imagery metadata.

- For the creation, processing and interchange of standardized and custom metadata for digital documents and data sets there is the Extensible Metadata Platform (XMP) ISO standard (ISO, 2012). XMP standardizes a data model, a serialization format and core properties for the definition and processing of extensible metadata. It also provides guidelines for embedding XMP information into popular image, video and document file formats.
- The IPTC Photo Metadata Standard (IPTC, 2019) is the most widely used standard to describe photos, because of its universal acceptance among news agencies, photographers, photo agencies, libraries, museums, and other related industries. It structures and defines metadata properties that allow users to add precise and reliable data about images.
- The MPEG-7 is a multimedia content description standard (ISO, 2002), with the description associated with the content itself, to allow fast and efficient searching for material that is of interest to the user.

Some work is being done for metadata definition regarding IoT devices (Milenkovic, 2015**)**. In addition, for technical data in WP4, message ID will be used (see Annex B).

2.2.5 Data sharing

This paragraph describes how data is shared within ARESIBO, including access procedures; outlines of technical mechanisms for dissemination and necessary software and other tools for enabling re-use; and describes how ARESIBO defines whether access is open or restricted to specific groups. It also covers the identification of the repository where information is stored: the ARESIBO password-protected cloud environment of the project (https://procloud.di.uoa.gr/).

All data that will be collected and stored during the ARESIBO project will not be freely/public accessible, i.e. no cloud services will be used for storing, if data are not anonymised/randomised/obfuscated. All data will be stored in the systems/storage/servers belonging to partner/s and access to these data will be granted by the respective ParDPO only to users working on project.

2.2.5.1 Access procedures

Due to the sensitive nature of some of the data and information relevant for ARESIBO, data security is of vital importance and an important aspect to consider is who can access the data. In case of datasets that should not be publicly accessible, a control mechanism is established including some of the below features:

- Authentication systems that limit real access only to authorized users.
- Procedures to monitor and evaluate all the access requests.

In case the dataset cannot be shared, the reasons for this should be mentioned (e.g. security-related, ethical, protection of personal data, intellectual property, commercial, privacy-related). Each time a new dataset is deposited, the consortium decides on who can access the data, upon prior approval of the DPO and PSO (see below para 2.2.2.2). Anonymised and aggregated data can be made freely available to everyone, whereas sensitive and confidential data is only accessed by specific authorized users under signed disclosure agreements.

Depending on the level of sensitivity of the data, special policy actions should be applied such as enforcing encryption of the content, secure communication, mailing list management and user access control.

- All working files such as deliverables, reports, presentations, spread sheets and alike should be uploaded into the secure password protected repository. As such repository ARESIBO project members have adopted the Procloud platform (https://procloud.di.uoa.gr/), which conforms to ISO/IEC 27001:2013 requirements on information security.
- Encryption of sensitive data is performed with the use of ZED! software. Functionality of ZED! software is further described in section 2.3.2.1 'Handling Sensitive Information'. Every encrypted file is password protected.
- Secure communication channels will be used by partners for exchange of data sets collected during project trials or field tests. For instance, Virtual Private Network (VPN) based communication software such as OpenVPN will be utilized.
- Exchange of electronic messages between project partners is organized on the basis of mailing lists, which are created and management separately for each work package. So every project partner can receive only emails that are relevant to the work package where the partner participates.
- User access to project files and folders on ARESIBO project platform is controlled through the creation of user groups per work package depending on partner's involvement. Filtering of access rights is done at user group level within the Procloud platform.

2.2.5.2 Methods for data sharing and contribution to the Open Research Data Pilot

Most of the data collected by technical WPs for the development and testing of the ARESIBO solutions (e.g. sensor data, voice and video streams, etc.) will be used only by partners in the implementation of the project. Most of these data will be sent through the Kafka message bus to be consumed and if needed further processed by the ARESIBO components. Some of this data will be also stored in a NoSQL database.[6] Details will be provided in the second version of the DMP.

Under Horizon 2020, beneficiaries of European Research Council (ERC) grants must ensure open access (free of charge, online access for any user) to all peer-reviewed scientific publications relating to its results. In the context of research and innovation, 'scientific information' refers to research data (data underlying publications, curated data and/or raw data). ARESIBO consortium is committed to Open Access, taking into consideration the need to balance openness and protection of scientific information, commercialisation and Intellectual Property Rights (IPR), privacy concerns, security as well as data management and preservation questions.

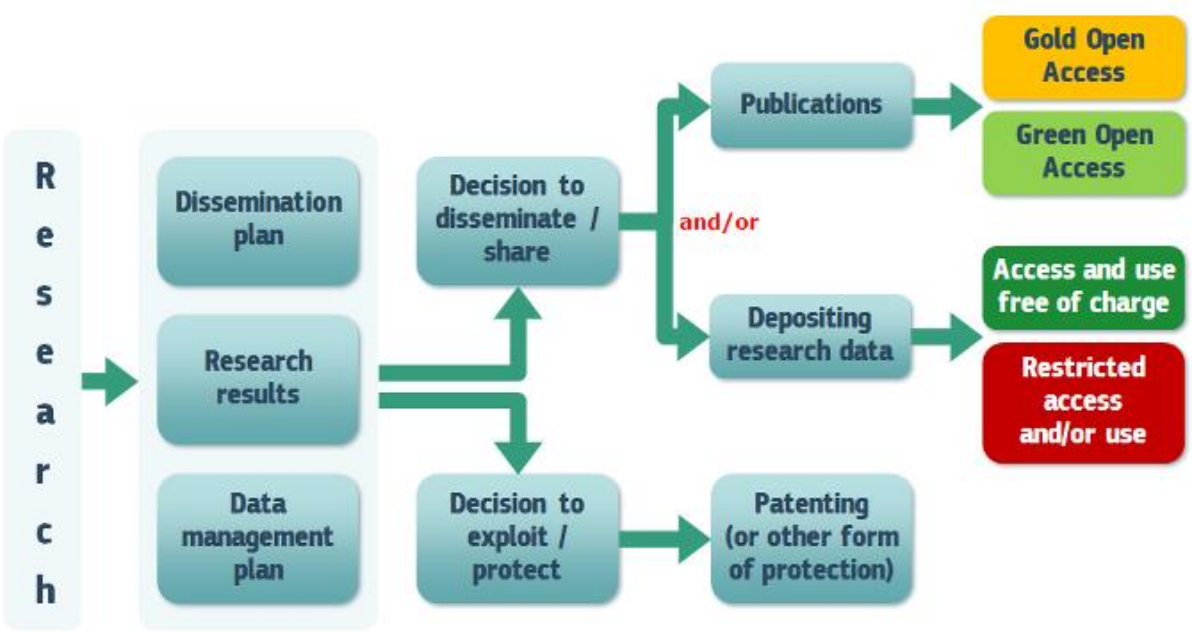
Therefore, it is understood that 'Open Access' does not imply an obligation in ARESIBO to publish its research results in open ('Green' and 'Gold' Open Access schemes), the publishing of data for ARESIBO is on a voluntary basis by the stakeholders, and in full alignment with the IPR and the patenting ARESIBO activities.

WP 8 (Dissemination and Exploitation), led by Intelligence for Environment and Security (IES) is specifically dedicated to the collection of data which can be made publicly available and disseminated to specific target audiences, either via the project website

[6] NoSQL database is an approach to database design that provides flexible schemas for the storage and retrieval of data beyond the traditional table structures found in relational databases. See "NoSQL Databases Explained". https://riak.com/resources/nosql-databases/index.html?p=9937.html#:~:text=NoSQL%20is%20an%20approach%20to,database%20management%20systems%20(RDBMS).&text=Relational%20databases%20rely%20on%20tables,use%20more%20flexible%20data%20models.

https://aresibo.eu/, the social media accounts (https://www.facebook.com/aresiboEU, https://twitter.com/aresiboEU, and https://www.linkedin.com/company/aresiboeu/) and specifically targeted dissemination activities (such as scientific publications, articles, presentations etc.).

Figure 5: Open Access to Scientific Publications and Data for Dissemination and Exploitation



Source: https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/open-access_en.htm

ARESIBO DMP is aligned to the above, aiming to contribute data to the open research pilot (ORDP). Data sets which are candidates for sharing will be carefully assessed to ensure that:

- They are not confidential, and do not include personal or commercially sensitive information according to GDPR.
- Permission from the relevant stakeholders and/or data subjects has been obtained.
- Sharing the data does not damage exploitation or IP protection prospects.

Specific data selected and considered as eligible for public distribution, will be disseminated, according to the DoA, through a variety of mediums and channels, including:

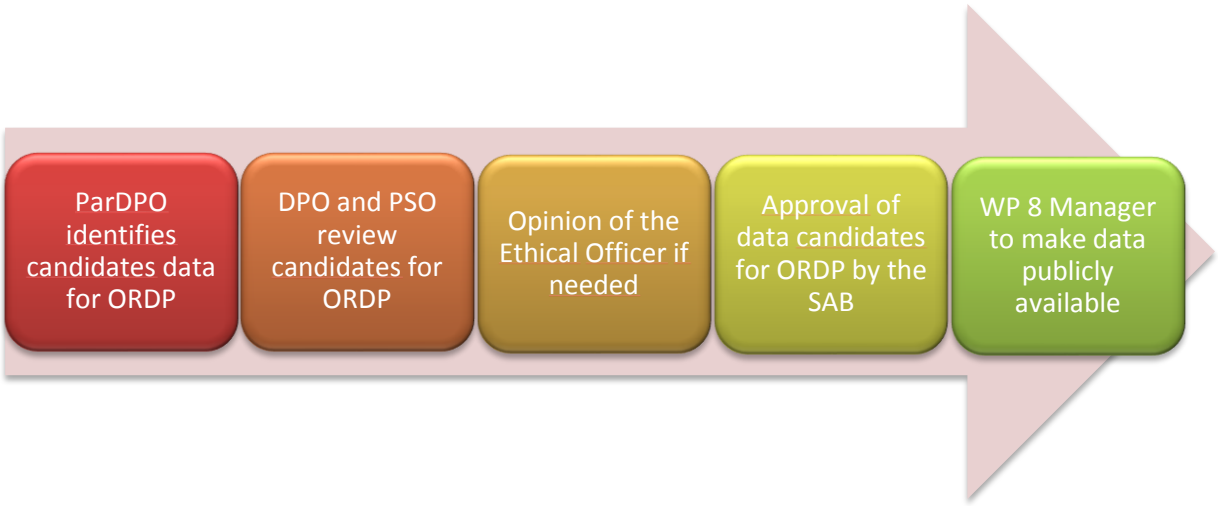
- Scientific papers in conferences and peer-reviewed journals;
- Interest groups created by the partners of the project;
- Dissemination though the dissemination and exploitation channels of the project to attract more interested parties.

The process for the selection of data contributing to the ORDP will follow these steps (as detailed in Figure 3 below):

1. Datasets in ARESIBO originated from the different stakeholders in different work packages (WPs), are reviewed by the relevant ParDPO who will identify candidates for contribution to the ORDP;
2. The DPO and PSO will review the ORDP candidate data and submit the list for approval to the Security Advisory Board (SAB);
3. Wherever needed, the opinion of the Ethical Officer will be requested;

4. Final approval of data candidates for ORDP will be granted by the SAB.

Fig. 6 Selection of data contributing to the ORDP



Where appropriate, data are embargoed to support IP protection or the exploitation time line for its release.

The DPO and the WP8 Manager will identify the modalities through which the non-restricted data can be made available for the public audience. The project website will be the key tool for the project communications. In addition, appropriate repositories will be considered for storing the results of the project and providing access to the scientific community, such as OpenAIRE[7] and Zenodo.[8] The Project Management Board (PMB) will decide which platform will be used.

2.2.6 Data storage, archiving and preservation

Each partner of ARESIBO organizes and stores data internally in the systems/storage/servers belonging to partner/s, transforming the data to knowledge assets, susceptible of being further disseminated within the consortium, if cleared by the DPO and the SAB.

Although little data will be preserved after the end of the project, ARESIBO will envisage procedures for long-term preservation of the data, providing Indication of how long the data should be preserved, what is its approximated end volume, what the associated costs are and how these are planned to be covered. All stored data will be preserved by the ARESIBO partners up to 2 years after the end of the project. Preservation procedures will be described in the second and final version of the Data Management Plan.

Raw, generated or collected/processed data or meta-data from ARESIBO project will be preserved and archived. The entire storage data set is archived in the ARESIBO password-secured storage platform, at least until the end of the project. The files containing the datasets are usually versioned over time. Also, the datasets are automatically backed up on a nightly and monthly basis.

[7] https://www.openaire.eu/
[8] https://zenodo.org/

2.3 ARESIBO data protection and security policies

Data protection and issues related to security are, as mentioned, two major aspects of the data governance, constituting the second pillar of the DMP which will be analysed in this section.

2.3.1 Protection of personal data

The protection of personal data is of major importance for the ARESIBO research and will be managed in T1.4 “Legal, Ethical and Social Issues management” and supervised by the ARESIBO Ethical Manager, in collaboration with the Project Manager and the DPO. ARESIBO research is not aimed at the collection or processing of any personal data. However, during the project events (such as meetings, workshops and demonstrations/tests), pictures and movies will be taken to support the dissemination and reporting actions. To comply with the European laws protecting privacy right, the participant of the meetings will be requested to sign a consent form where they will notify their acceptance or refusal to the publication of images where they appear (as detailed in Deliverable 9.2).

In any event, ARESIBO does not involve the collection and/or processing of sensitive personal data (such as health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction).

In the case where any activity implies processing of data that can relate to identified or identifiable persons, this activity will be strictly governed by EU General Data Protection Regulation (GDPR) 2016/679, whereby, *inter alia*, the data controllers and processors are accountable for the data processing operations. With regards to collection and storage of information with possible personal data, as mentioned, each host institution has appointed a ParDPO, whose contact details will be made available to all data subjects involved in the research.

Anonymisation/pseudonymisation techniques will be used in case of personal data are gathered in the research activities or testing of the ARESIBO solutions. Such techniques will be described in the deliverable with the analysis of the relevant information.

In any case, all personal data that will no longer be used for project purposes will be deleted as soon as possible. All personal and sensitive data will be made anonymous as soon as possible. At the end of the project, only data accurately anonymised will be susceptible of being stored in an open repository.

During the requirements analysis phase (Task 2.1), the data gathered through structured questionnaires or interviews[9] will be anonymised before they are further processed by the consortium members. The data collection involved only end users’ organisations partner in the project, i.e. end users representing land border FBG, SPP and BDI; and end users focusing on sea border MARINHA and HMOD.

Consent forms are and will be used across all stages of the project, including interviews, workshops, seminars, demos, etc.

[9] To collect the requirements, a structured questionnaire was submitted to all end-user organization. The questionnaire included mostly open-ended questions was sent to end users with the possibility either to collect the answers by interviewing a participant or by giving the template to the participant to be filled by themselves (see D2.1 User requirements and cognitive issues).

In T1.4 “Legal, Ethical and Social Issues Management”, the active involvement of citizens has been investigated to assess the acceptance of the system by the public audiences. Participatory models, methodologies and tools used for promoting stakeholders and citizens’ involvement will be used. Participants in these activities have been provided with the informed consent procedures and an informed consent form produced by WP9 Ethics (see Deliverable 9.2), and relevant nominal data will be anonymised.

The same process will be followed during the system’s evaluation stage. Among others, UAV-related data (video/image sequences) will be collected to support Project Use Cases (PUC), which implies the observation and tracking of participants. The ARESIBO consortium will clearly identify the privacy enhancing technologies that will be utilised to avoid people stigmatisation (in case of false positive alarms), when such technology will be in operation (i.e. use of blurring techniques in all faces detected in a scene during the remote collaboration of stakeholders in the field).

2.3.1.1 Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) has been undertaken under Task 2.3. DPIA is one of the specific processes mandated by the General Data Protection Regulation (GDPR). The GDPR states that organisations must carry out a DPIA where a planned or existing processing operation – “is likely to result in a high risk to the rights and freedoms of individuals”. DPIAs are particularly relevant to taking a privacy-by-design approach when introducing a new data processing system or technology. The ARESBIO DPIA consists of few stages: 1) Identification of the need for a DPIA; 2) Description of the information flow; 3) Identification of privacy and related risks; 4) Identification and evaluation of ethical values; 5) Recording the DPIA outcomes and integration of the DPIA outcomes into the project (in a specific report or report section).

The DPIA not only identifies privacy and related risk, but also evaluates some ethical and privacy values coming from key legal instruments, as the Charter of Fundamental Rights of the European Union; and European Convention for the Protection of Human Rights and Fundamental Freedoms.

A specific questionnaire has been developed by ISIG in October 2019, addressed to technical partners to understand how the information within the processing operation will be collected, stored, used and deleted. The results of this step were reported in D2.3.

The procedures and criteria that will be used to identify/recruit research participants will be dealt with within WP9. In particular, the informed consent procedures that will be implemented for the participation of humans will be described. Templates of the informed consent forms and information sheets (in) will be attached. Language and terms used in such documents will be simple and clear so as to be easily comprehensible to research participants.

Also, prior to the data collection, the opinion/approval by the Ethics Committee and/or for the research with humans will be requested. Copies of the opinion/approval will be submitted as a deliverable.

2.3.2 Security Issues

All organisations participating in ARESIBO have committed to comply with the Commission’s security rules and standards when handling any EU classified information (EUCI) as they are described in Commission Decision 2015/444. Specifically, all beneficiaries will comply with the Commission’s security rules and standards (i.e. Commission Decision 2015/444) when

handling any EUCI. ADS, the Project Coordinator, has signed the final security aspect letter provided by the European Commission in the course of the Grant Preparation.

EUCI is information that has been classified and marked, or its equivalent under a national classification system. Whenever ARESIBO consortium uses EUCI as background or results, this information will be marked according to Commission and national rules, but not greater than CONFIDENTIEL UE.

As the project deals with border security issues and critical information, it may raise security concerns. A major priority for the partnership is to secure the material collected or produced by partners in this research. For this reason, the Security Advisory Board (SAB) has been set up in order to address security issues and ensure the proper handling of sensitive and classified information.

The SAB consists of representatives appointed by FBG, HMOD, SPP, MARINHA, BDI, CBRA, and ISIG. In addition, all ParPSOs are part of the SAB. It will be responsible for auditing all security aspects of the projects, including in particular:

- the platform resilience to software attacks;
- the security aspects of the project;
- the information security of all deliverables and/or publications, taking into account privacy issues/data protection as well as the potential value of the released information to malicious attackers.

In support of the work of SAB, every project partner is committed to implement a process to assess the risks which might accompany the publication of a given deliverable from the internal point of view of the partner. SAB has to define the final dissemination level and specified group of recipients, taking into account the identified security risks as well as the interests of the Consortium partners. It will do so by communicating with the respective task leader of a deliverable as well as with the Project Officer appointed for the project ARESIBO.

The SAB meets annually or demand if security issues are detected by the consortium. The ARESIBO SAB is chaired by the ARESIBO PSO, who acts as single point of contact for all security aspects. He is responsible for leading and advising on all security matters relating to the ARESIBO project and chairing the Security Advisory Board of the project.

The PSO coordinates the review of all potential EUCI-related content and documentation, over the lifetime of the project and reports at the SAB and Project Management Board (PMB) meetings. Documents and materials with potential EUCI-related content will be included in the Security Classification Guide of the project.

As envisaged in section 6.1 of the DoA, a number of deliverables will be subject to limited dissemination (consortium only). Nonetheless, all the classified deliverables will also have a two-pager public version, approved by the SAB. This procedure could be reviewed to better support the dissemination objectives of the project. A preliminary ARESIBO Security Classification Guide was also provided in the DoA under section 6.2.2 (see table 1 below). In case any deliverable will need to be reclassified, prior approval by the European Commission shall be obtained.

Table 1 – Security Classification Guide

Production of Classified Foreground Information					
Subject	**Classification**	**Name**	**Responsibility**	**Date of**	**Comments including purpose of**

	Level expected			production	the actions and planned use
D1.3 "Intermediate Progress Report"	EU-restricted	ADS WP1 Partners	Main Author Contributors	M18	EUCI related to operational procedures is expected to be included in the deliverable. A reduced subset of this document containing no EUCI will be provided to the partners that do not have the required security clearance level.
D1.6.x "Requirements Traceability Matrix"	EU-restricted	IML WP1 Partners	Main Author Contributors	M06, M12, M20, M30, M34	EUCI related to operational procedures is expected to be included in the deliverable. A reduced subset of this document containing no EUCI will be provided to the partners that do not have the required security clearance level.
D2.1.x "User requirements and cognitive issues"	EU-restricted	FBG WP2 Partners	Main Author Contributors	M06, M22	EUCI related to operational procedures is expected to be included in the deliverable. A reduced subset of this document containing no EUCI will be provided to the partners that do not have the required security clearance level.
D2.2.x "Periodic report on implementation of security, data privacy and confidentiality requirements"	EU-restricted	ISIG WP2 Partners	Main Author Contributors	M11, M22	EUCI related to operational procedures is expected to be included in the deliverable. A reduced subset of this document containing no EUCI will be provided to the partners that do not have the required security clearance level.
D2.4 "Compliance with the EU Smart Border Package in pilot areas"	EU-restricted	ISIG WP2 Partners	Main Author Contributors	M16	EUCI related to operational procedures is expected to be included in the deliverable. A reduced subset of this document containing no EUCI will be provided to the partners that do not have the required security clearance level.
D1.6.x "CONOPS analysis, demonstration scenarios and evaluation metrics"	EU-restricted	MARINHA WP2 Partners	Main Author Contributors	M12, M24	EUCI related to operational procedures is expected to be included in the deliverable. A reduced subset of this document containing no EUCI will be provided to the partners that do not have the required security clearance level.
D3.4 "Data communication protocols and cyber-security"	EU-restricted	TEK-ASDS WP3 Partners	Main Author Contributors	M28	EUCI related to operational procedures is expected to be included in the deliverable. A reduced subset of this document containing no EUCI will be provided to the partners that do not have the required security clearance level.
D3.5 "Voice and video communication tool for border security operations"	EU-restricted	VIASAT WP3 Partners	Main Author Contributors	M28	EUCI related to operational procedures is expected to be included in the deliverable. A reduced subset of this document containing no EUCI will be provided to the partners that do not have the required security clearance level.
D4.3.x "Simulation environment and Decision Support for Coast- and Border-Guards"	EU-restricted	CMRE/I4ES WP4 Partners	Main Author Contributors	M14, M28	In case EUCI related to operational procedures will be included in the deliverable it is proposed to manage the classified part, when possible, in classified annexes with the intent to facilitate the dissemination of the results For what concerns the

					simulation part, these deliverables will present the characteristics of the interoperable simulators that will be integrated with the training environment and serious game In particular the reports will include - the description of the simulators, that does not require any operational sensitive detail. - And the description of non-classified scenarios modelled to run realistic scenarios, again, does not require any sensitive information. If there was any requirement to run classified simulated scenario, a Simulation Manager will be delivered to the partner involved in the execution of the simulation and EU_RES Annexes could be delivered by the involved partner and attached to the reports to include sensitive information.
D5.2.x "AR Tools on Field Operations"	EU-restricted	UBI WP5 Partners	Main Author Contributors	M14, M28	EUCI related to operational procedures is expected to be included in the deliverable. A reduced subset of this document containing no EUCI will be provided to the partners that do not have the required security clearance level.
D5.3.x "AR Tools on C2"	EU-restricted	VTT WP5 Partners	Main Author Contributors	M14, M28	EUCI related to operational procedures is expected to be included in the deliverable. A reduced subset of this document containing no EUCI will be provided to the partners that do not have the required security clearance level.
D5.4 "Time-Based Visualization in AR"	EU-restricted	VTT WP5 Partners	Main Author Contributors	M28	EUCI related to operational procedures is expected to be included in .the deliverable. A reduced subset of this document containing no EUCI will be provided to the partners that do not have the required security clearance level.
D5.5 "Serious game for user training"	EU-restricted	CMRE WP5 HMoD, BDI, FBG, MARINHA, SPP	Main Author Contributors	M28	These deliverables will present the characteristics of the training environment and the serious game. In particular the reports will include The description of the training scenario will be delivered in WP7 reports. If there was any requirement to include classified simulated training scenario, the simulation manager will be delivered to the trainers and EU_RES Annexes could be attached to the main document by the involved partner to include any sensitive information.
D7.1 "Evaluation methodology report"	EU-restricted	MARINHA WP7 Partners	Main Author Contributors	M30	EUCI related to operational procedures is expected to be included in the deliverable. A reduced subset of this document containing no EUCI will be provided to the partners that do not have the required security clearance level.

In addition to the protection of personal data, dual-use items in the sense of Regulation 428/2009 should be considered and handled by the project. In particular, some of the ARESIBO technologies or research dimensions (e.g., automated use of unmanned vehicles, visual detection of targets) may be considered as dual-use research since they could be applied in both civilian and military applications. However, it is worth mentioning that all ARESIBO technologies have been designed for the civilian market (i.e., to secure public safety) or used successfully in the civilian applications domain. In any case, a strict and clear declaration comes from the ARESIBO consortium that none of the considered technologies will be applied for military purpose.

Particular attention will also be devoted throughout the project implementation to the issue of confidentiality. All consortium members have agreed that any material of confidential nature supplied to the ARESIBO project will remain strictly for the information of the project members and will not be disclosed to any other party without the explicit authorization from the information owner. Section 10 - Non Disclosure of the Consortium Agreement governs in detail aspects related to confidential information.

In addition, access to EUCI will be provided only to parties with the proper level of Security Clearance (Facility and/or personal). All details related to IPR handling and confidentiality will be explicitly defined in the CA that will be compiled and signed for the project purposes. EU-classified information will not be shared with non-EU External Advisory Board Member, to ensure that EU- classified information is share only within EU Member States. In the case of experts from Switzerland, the PSO in conjunction with the SAB will identify in which deliverables they are involved and if there is a need for sharing this type of information, following the “need to know” principle.

2.3.2.1 Handling Sensitive Information

An expected level of classification was proposed at the beginning of the project, the information used in the context of the ARESIBO research, either as background or results, will be classified by the responsible task leader/WP leader/or Project coordinator according to the “Guidelines for the classification of information in research projects” Directive of European Commission. Consultation of the SAB can be pursued in special cases, if needed.

Beneficiaries that need to access EUCI in order to perform activities necessary for the implementation of the project should fully comply with the security rules and standards of European Commission when handling any EU classified information as they are given in Commission Decision 2015/444. The exact security measures that could be taken by those beneficiaries that need to access EUCI are described in the EUCI Regulatory Framework of EC. One of the requirements that should be satisfied before accessing or storing EUCI is the acquisition of a Personal Security Clearance (PSC) and Facility Security Clearance (FSC), respectively, even if the current proposed highest level of classification is EU restricted that does not require PSC of FSC.

All data that are restricted will be encrypted and password protected. The consortium agreed to adopt ZEDPRO, a professional version of Zed software, for the encryption of data. ZED![10] is a software tool for encryption of sensitive and personal data. ZED! guarantees data protection and confidentiality for exchange and storage. The Enterprise version of ZED! software has passed through full NATO evaluation and was approved by the Council of the European Union. Professional ZED! version is not certified nor qualified however it is suitable

[10] https://www.zedencrypt.com/

for exchange of sensitive files.[11] The tool uses AES 256 encryption algorithm and stores data in a secure container protected by a password or standard certificate. The certificate with a private key can be stored in .pfx or .p12 PKCS#12 files, in Windows CSP container, written on a PKCS#11 smart card or USB device.

ZED! secure container has '.zed' file extension and supports data compression like standard archivers such as ZIP, RAR, ARJ etc. Secure data container is produced in the form of 'FileName.zed' file.

ZED! is not a platform for secure data management so in practice every file or folder should be encrypted before being uploaded to password-protected cloud environment of the project (https://procloud.di.uoa.gr/)where project files are kept. Access management is done by the super user at folder or file level inside the secure container. It means that the main user who created the secure container should maintain the access list inside it. The list of allowed users can be built upon a user/password combination or users' digital certificates.

As consortium members have different access levels depending on their role and contribution, it would be advisable for every party to generate its own digital certificate for the purpose of access management inside ZED! secure containers.

Decryption procedure over the secure container is performed by the receiving party on its computer with the use of a user/password combination or with a personal private key. The software is multiplatform and is available for 32 and 64 bits versions including Windows 7, 8.1, 10, Linux Ubuntu, CentOS and macOS 10.13 High Sierra, 10.14 Mojave, and 10.15 Catalina.
In general, ZED! software would work nicely with small data sets like deliverables, annexes and other working documents. From FAIR Data Management perspective, ZED! can ensure certain level of Data security and is compliant with the DMP component number 4.

2.3.2.2 Personal and Facility Security Clearance

As mentioned above, all partners dealing with classified information have appointed the required ParPSO. Only partners will the relevant Personal Security Clearance (PSC) will be given permission to access EUCI, when required. In addition, a partner will be allowed to store EUCI only if the same partner facility complies with EU rules. The same process will stand for data, documents and meetings that may take place throughout the lifetime of the project.

All the processes related to security issues will be supervised and regularly checked by the PSO, with the support of the SAB, whenever this is needed.

In case a partner that does not comply with the required security conditions needs to access EUCI for activities related to the implementation of an envisaged task, upon approval of the relevant ParPSO, an "Unclassified" version of the information will be provided to him/her. In case of meetings or participation in project discussions where EUCI is needed to be discussed, the respective partner will not be able to attend the meeting or the discussion unless a PSC is provided to the Project Security Officer.

[11] https://www.zedencrypt.com/download

2.4 ARESIBO privacy principles

2.4.1 Personal Data

ARESIBO follows the data quality principles established in the GDPR. When assessing the privacy and related risks it assesses the level of risk existing for each of the data quality principles. Therefore, ARESIBO pays particular attention to the following principles:

1. Personal data must be processed fairly, lawfully and in a transparent manner;
2. Purpose limitation and specification;
3. Data minimization (adequate, relevant, accurate, and limited to the minimum necessary in relation to the processing purpose, retention periods);
4. Personal data must be processed under the responsibility and liability of the controller, which is also responsible for compliance with the GDPR (principle of accountability);
5. Principle of transparency (data controller-data subject/supervisory authorities).

The data processors within the project need to pay particular attention to their responsibilities (established in the GDPR):

1. Processors should provide sufficient guarantees of security;
2. Processors have direct obligations for implementing appropriate technical and organisational measures;
3. Processors may be ordered by the supervisory authority to comply with data subjects' requests to exercise their rights.

ARESIBO will not collect or process personal data. However, during the project events (meetings, workshops and demonstrations/tests), pictures and movies will be taken to support the dissemination and reporting actions. To comply with the European laws protecting privacy right, participants to such meetings and events will sign a consent form (accompanied by an Information Sheet - see D2.1) where they will notify their acceptance or refusal to the publication of images where they appear. The consent form will be customised for each type of event.

In research tasks such as for instance during the requirements analysis phase, the requirements and data are gathered through questionnaires or interviews which have been anonymised before being further processed by the consortium members. The same process will be followed during the project evaluation stage.

Handling data (personal and/or anonymized) follows several steps: 1) collection of data; 2) processing of data; 3) storing of data; and 4) transfer of data. Each of these steps is to be properly explained by all project partners carrying them out throughout the project lifetime. In D2.3, the initial assessment (the second step of the ARESIBO DPIA) which included the description of the information flow was reported and structured following these four steps. The assessment will continue with the same structure and methodology.

The project's Ethical Manager will coordinate with the DPO for all matters raising privacy and ethical concerns.

2.4.2 Commercial data

According to Section 10 of the Consortium Agreement, ARESIBO partners are committed to a non disclosure clause.

2.5 Conclusions

Task 1.6 has developed the present Data Management Plan to guide partners in the data management life cycle for all data that will be collected, processed or generated by the project. The DMP designs the data governance and highlights the role of different actors involved at central as well as at partner level. It focuses on the importance of security issues and procedures governing classified data collection and sharing.

A second and final version of the present document will be produced at M36.

Annex A: Consortium Partners' Data Protection Officers and Security Officers [internal distribution only]

Annex B: Data Summary by WP

WP 1 – Project Management

WP 2 – Requirements analysis and pilot use-cases

DPM Component	Issues to be addressed
Data Summary	What is the purpose of the data collection/generation in WP? What types and formats of data will the project generate/collect? Will you re-use any existing data and how? What is the origin of the data? What is the expected size of the data? To whom might it be useful ('data utility')? Are the data produced and/or used discoverable with metadata, identifiable and locatable by means of a standard identification mechanism (e.g. persistent and unique identifiers such as Digital Object Identifiers)? What naming conventions are followed? Will search keywords be provided that optimize possibilities for re-use? Do you provide clear version numbers? What metadata will be created?

Answers:

In **Task 2.1** and **Task 2.2** data is collected for defining the end-user requirements for the ARESIBO solution. Specific data sets are questionnaires and notes and minutes of workshops and meetings stored in pdf and .xlsx forms. The data is collected from the end-user organisations of the project. As the data is classified and stored in secure environment at FBG it can't be utilised by third parties.

Metadata or keywords for reutilisation are not utilised.

In **Task 2.3** datasets are collected for the definition of security, data privacy and confidentiality requirements within the project. Data are collected from all project partners.

Specific data sets are:
- Notes and minutes of workshops, meetings;
- Questionnaire responses (excel);

Files are anonymised and stored in .xlsx format.

Size: N/A

In **Task 2.4** datasets are collected for the definition of Ethical, legal and social requirements for border security.

Specific datasets are:
- Notes and minutes of the workshops, meetings;
- Questionnaire responses (excel), from:
  - End-users (on cross-border practices);
  - Citizens (on the citizens' acceptance and perception of security and monitoring technologies).

Files are anonymised and stored in .xlsx and .sav formats.

Size: N/A

In **Task 2.5** datasets are collected for understanding and characterization of the concept in maritime border security operations, the adoption of end-users' requirements in the design of Use Cases and characterization

of testbed facilities to develop Use cases and design demo/test scenarios.

Types of data: interviews, workshops, questionnaires with SME, technical reports (assets and testbed descriptions), cartographic information, climatology.

Formats: hand notes, reports, audio recordings, questionnaires' answers data files (MS Excel)

Re-use of existing data Data:

- regarding the environmental conditions of the testbeds, for instance:
    - Satellite imagery from google earth
    - Nautical charts
    - Weather reports, weather stations data reports
- It is used to support the design of the scenarios and use-cases scripts
- Information from the environmental conditions is collect from Opensource, proprietary or commercial sources.

Size of the data varies from a few kb such as text reports to Mb such as audio recordings and chart data.

Data might be useful for:

- End-users for CONOP analysis and development of new concepts of operations
- Academia to support research/studies about:
    - Impact/interaction with novel technologies
    - Collaborative Decision-making in complex scenarios
    - Situational awareness
    - Social acceptance of new forms of border control operations
- Industry to support the design and development of new technologies used by end-user in maritime border control.

In **Task 2.6** Data collected or generated will be used for the management of Task 2.6.

What types and formats of data will the project generate/collect?

- Notes and minutes of the workshops and meetings.
- Data will be in .docx, .pdf, .ppt .xlsx, or Google Docs form and they will be stored in ARESIBO cloud repository.

Will you re-use any existing data and how?
Data collected or generated will be used for the management of Task 2.6.

What is the origin of the data?
The data originate from the partners participation in meetings, presentations, workshops, teleconferences.

What is the expected size of the data?
Several Mbytes.

To whom might it be useful ('data utility')?
To the project partners.

Are the data produced and/or used discoverable with metadata, identifiable and locatable by means of a standard identification mechanism (e.g. persistent and unique identifiers such as Digital Object Identifiers)?
No.

What naming conventions are followed?
The naming conventions follow the Grant Agreement naming of documents (e.g. D2.8, Task 2.6).

Will search keywords be provided that optimize possibilities for re-use?
No.

Do you provide clear version numbers? Yes. What metadata will be created? File properties as saved in its electronic form.

WP 3- Augmented Communication and Sensing for integrated situation awareness

WP 4 – Augmented Intelligence for integrated situation awareness

DPM Component	Issues to be addressed
Data Summary	What is the purpose of the data collection/generation in WP? What types and formats of data will the project generate/collect? Will you re-use any existing data and how? What is the origin of the data? What is the expected size of the data? To whom might it be useful ('data utility')? Are the data produced and/or used discoverable with metadata, identifiable and locatable by means of a standard identification mechanism (e.g. persistent and unique identifiers such as Digital Object Identifiers)? What naming conventions are followed? Will search keywords be provided that optimize possibilities for re-use? Do you provide clear version numbers? What metadata will be created?

Answers:
From a technical point of view, a first version of the datatypes that will be created and/or processed under the scope of WP4 is specified in deliverable D4.1 “Data representation model V1”. In this deliverable, the format and the fields of the considered messages are defined in detail. It is expected that these datatypes will be finalised in deliverable D4.2 which constitutes the second version of the ARESIBO data model.
A summary of the data can be found below:
- UxV plans and waypoints
- Commands and actions
- UxV Missions
- Mission status
- Telemetry Data
- Area-of-Interest (AoI) data
- Data about Aerial/Ground/Underwater Vehicles
- Weather data and environmental conditions
- Sensor streams and sensor data
- Data about XR (AR/MR/VR) devices
- Video detection data
- Alert data
- Geospatial data
- Decision support actions
- Voice streams
- Video streams

Size of data varies from a few bytes (e.g., a sensor value) to several Mb or even Gb such as video streams. The format of the data will be based on JSON (apart from videos).

Most of the above data will be sent through the Kafka message bus to be consumed and if needed further processed by the ARESIBO components. Some of this data will be also stored in a NoSQL database.

From an administrative and non-technical standpoint, WP4 will create data about the regular meetings that

take place including data about the WP4 telcos (e.g., participating entities, minutes of the discussion, PowerPoint presentations). Such data are regularly uploaded to the password-protected cloud environment of the project (https://procloud.di.uoa.gr/). Size of data varies from a few bytes (e.g., a sensor value) to several Mb such as multimedia presentations or video tutorials. The format of the data will vary from plain text files to PowerPoint presentations, Excel sheets, Docx documents and PDF files.

Will you re-use any existing data and how?
Technical data will be re-used during tests and trials. Administrative data will be used for reporting and coordination of the work.

What is the origin of the data?
The project partners and the hardware that will be used (AR devices, sensors, UxVs, etc.).

To whom might it be useful ('data utility')?
To the project partners.

Are the data produced and/or used discoverable with metadata, identifiable and locatable by means of a standard identification mechanism (e.g. persistent and unique identifiers such as Digital Object Identifiers)?
Technical data: Message IDs will be used. Administrative data: No.

Will search keywords be provided that optimize possibilities for re-use?
No.

Do you provide clear version numbers?
Yes. File versioning will be normally used.

What metadata will be created?
File properties.

WP 5 – Requirements analysis and pilot use-cases

DPM Component	Issues to be addressed
Data Summary	What is the purpose of the data collection/generation in WP? What types and formats of data will the project generate/collect? Will you re-use any existing data and how? What is the origin of the data? What is the expected size of the data? To whom might it be useful ('data utility')? Are the data produced and/or used discoverable with metadata, identifiable and locatable by means of a standard identification mechanism (e.g. persistent and unique identifiers such as Digital Object Identifiers)? What naming conventions are followed? Will search keywords be provided that optimize possibilities for re-use? Do you provide clear version numbers? What metadata will be created?

Answers:
In WP5 datasets are defined in “D5.1 AR Data Interface V1”. More detailed information could be found in deliverable. Data will transfer and stored in ARESIBO Kafka server and database.
Here is summary of data to handled and stored:

(1) Video from external devices such as UxVs or cameras, offline videos from various sources to get better situation awareness.
(2) Image: Still images from various sources and other stake holders such as Tactical Commander, C2, UxVs and external cameras.
(3) Sensor data: Information from various sensors such as motion sensor, radar information.

(4) NATO symbols: Standard symbols such as MilSTD2525C or NATO App6b
(5) Other symbols: Remaining symbols will be specified in v2 based on the experiences from the initial trial.
(6) Audio: Audio files containing information on the task
(7) Voice Stream: Real time stream between various sources such as Tactical Commander, C2 and other units.
(8) Video Stream: Real time stream between various sources such as Tactical Commander, C2 and other units.
(9) Maps: Standard maps with meta data which could be online or offline
(10) Location of various objects: Location information of various relevant objects.
(11) Textual Notes: Notes that contain instruction or information from previous similar incidents.
(12) Data from RADAR: External RADAR data that is relevant for the task.
(13) Data from Law enforcement registers: External data from registers that can support situational awareness of the User.
(14) Data logging model, where data could be analyzed after the mission and/or used evidence for illegal activities.
(15) Live 3D elements for teams along with identified objects or targets (deep real-time image analysis and instant population of the map with identified objects)
(16) Interrogations of POI/AOI or targets with the automated video visualization of the place and tools for sending target and AOI positions to the field officers

Other data sets:

- Notes and minutes of bi-weekly telcos as pptx in project clouds
- Questionnaire responses as pptx in project clouds

WP 6 Integration of ARESIBO Platform

WP 7– Augmented Intelligence for integrated situation awareness

DPM Component	Issues to be addressed
Data Summary	What is the purpose of the data collection/generation in WP? What types and formats of data will the project generate/collect? Will you re-use any existing data and how? What is the origin of the data? What is the expected size of the data? To whom might it be useful ('data utility')? Are the data produced and/or used discoverable with metadata? Are the data identifiable and locatable through standard identification mechanism (e.g. persistent and unique identifiers such as Digital Object Identifiers)? What are the conventions followed? Will search keywords be provided that optimize possibilities for re-use? Do you provide precise version numbers? What metadata will be created?

Answers

What is the purpose of the data collection/generation in WP?

The purpose of the collected data is to support the project's metrics framework that forms the base to assess the established KPIs.

Over the nine field tests, the same metrics will also provide insights over the stage development of each technical modules and system integration. This assessment will support the partners in the revision of their tasks and enhancement of both the functional modules and user requirements, through several iterative

processes.

What types and formats of data will the project generate/collect?

From a technical point of view, a first version of the data types that will be created and/or processed under the scope of WP7 is the same as the ones specified in deliverable D4.1 “Data representation model V1” of WP4. In this deliverable, the format and the fields of the considered messages are detailed. After one iterative cycle, the final version of these data types will be published in deliverable D4.2.

A summary of the data can be found below:

- UxV operational data:
- Route plan:
  - waypoints (X;Y;Z)[m]; (lat, long, alt)[WGS84)
  - ETA[yyy;mm;dd;hh;mm;ss)[UTC]
  - ETD [yyy;mm;dd;hh;mm;ss)[UTC]
  - Speed [units: km/h; knots; m/s]
  - Course[True north; magnetic]
- Base
  - waypoints (X;Y;Z)[m]; (lat, long, alt)[WGS84)
  - moving
    - True Speed(SOG)(00,00) [units: km/h; knots; m/s]
    - Course (COG)(000,0) [True north; magnetic]
    - Route plan
- Commands and actions
  - Speed[units: km/h; knots; m/s]
  - Course [True north; magnetic]
  - Heading [true north; magnetic]
  - Rate of turn (00,0) [degrees / seconds)
  - Acceleration
  - Vertical acceleration
  - Sensors commands
- Level of interoperability, Rx/Tx of telemetry, control payload data (from indirect data links from UxV to other sources to full control of GCS)
- Level of automation (from no automation to fully autonomous)
- UxV Missions
  - Area limits (polygon) [WGS84]
  - Elevation limits [m]
  - Depth limits (m)
  -
- Mission status
- Telemetry Data
  - Position (X;Y;Z)[m]; (lat, long, alt)[WGS84)
  - True Speed (SOG) (00,00) [units: km/h; knots; m/s]
  - Speed through water(00,00) [units: km/h; knots; m/s]
  - Endurance/autonomy
  - Energy usage
  - Course (COG) (000,0) [True north; magnetic]
  - Heading (000,0) [True north; magnetic]
  - Pitch
  - Roll
  - drift
- Area-of-Interest (AoI) data
- Data about Aerial/Ground/Underwater Vehicles
- Weather data and environmental conditions
  - Wind
  - Air temperature
  - Water temperature
  - Humidity
  - Cloud base levels
  - Currents

    - Tide
    - Swell
    - Wave period/direction
    - Pressure
    - visibility
- Sensor streams and sensor data
- Data about XR (AR/MR/VR) devices
    - 2D/3D
    - Single / dual
    - Field of view
    - Display type
    - Command interaction
        - Hand gestures
        - Voice
        - Clicker
        - positional tracking sensors
    - Resolution
    - Weight
    - Autonomy
    -
- Video detection data
- Alert data
- Geospatial data
- Decision support actions
- Voice streams
- Video streams

Size of data varies from a few bytes (e.g., a sensor value) to several Mb or even Gb such as video streams. The format of the data will be based on JSON (apart from videos).
All the above technical data will be exchanged during field tests, deployments and demos, which are the core business of WP7.

Most of the above data will be sent through the Kafka message bus to be consumed and if needed, further processed by the ARESIBO components. Some of this data will also be stored in a NoSQL database.

From an administrative and non-technical standpoint, WP7 will create data about the regular meetings that take place, including data about the WP7 telcos (e.g., participating entities, minutes of the discussion, PowerPoint presentations). Such data are regularly uploaded to the password-protected cloud environment of the project (https://procloud.di.uoa.gr/). Size of data varies from a few bytes (e.g., a sensor value) to several Mbytes such as multimedia presentations or video tutorials. The format of the data will vary from plain text files to PowerPoint presentations, Excel sheets, Docx documents and PDF files.

The most important data that will be created and handled in WP7 are the personal data related to information gathered during the field trials (e.g. images, videos) and the data provided in the questionnaires that will be filled in by the users (operators) of ARESIBO to assess and evaluate the system.
Personal data collected will be anonymized, encrypted and sanitized by proper anonymization/pseudonymization techniques. All data that are restricted will be encrypted and password protected. The consortium agreed to adopt ZedPro software for the encryption of data.

Anonymisation/pseudonymization techniques will be used in case of personal data are gathered in the research activities or testing of the ARESIBO solutions. Such techniques will be described in the deliverable with the analysis of the relevant information.

In any case, all personal data that will no longer be used for project purposes will be deleted as soon as possible. All personal and sensitive data will be made anonymous as soon as possible. At the end of the project, only data accurately anonymized will be susceptible to being stored in an open repository.

During the evaluation of human factors and UX (Task 7.1), the data gathered through structured

questionnaires or interviews will be anonymized before they are further processed by the consortium members. The same applies to Tasks 7.5 and 7.6, where data collection involves mainly end-user organizations partners in the project, for land and maritime border surveillance.

Consent forms will be used, and relevant nominal data will be anonymized across all stages of WP7, including interviews, KPIs measurement, evaluation metrics, end-users self-assessment and EAB members external evaluation.

The same process will be followed during the system's evaluation stage. Among others, UAV-related data (video/image sequences) will be collected to support Project Use Cases (PUC), which implies the observation and tracking of participants. The ARESIBO consortium will clearly identify the privacy enhancing technologies that will be utilized to avoid people stigmatization (in case of false positive alarms), when such technology will be in operation (i.e. use of blurring techniques in all faces detected in a scene during the remote collaboration of stakeholders in the field).

Will you re-use any existing data and how?
Technical data will be re-used during tests and trials. Administrative data will be used for reporting and coordination of the work. Personal data will be used for system evaluation and assessment.
Cartographic data from test bed location to be used as base maps.

What is the origin of the data?
The project partners, the end-users operators, the EAB members and the hardware that will be used (AR devices, sensors, UxVs, etc.).
Survey data collected from different stakeholders to assess the ethical and societal perceptions and impacts of the proposed approach for border security operations.

To whom might it be useful ('data utility')?
To the project partners and the final ARESIBO system assessment.
LEA agencies, EU commission and governments to review political strategies and guidance for border security operation within EU member states.
Security companies focused on the protection of critical infrastructures, land and sea.
Data on the use and assessment of AR devices might be useful for academia and research to develop these technologies further.
Data on the assessment of operators training for technical use of the different AR devices and decision support tools, applying serious games, can be of the interest of training and education organization.

Are the data produced and/or used discoverable with metadata, identifiable and locatable by means of a standard identification mechanism (e.g. persistent and unique identifiers such as Digital Object Identifiers)?
Technical data: Message IDs will be used. Administrative data: No.Personal data: No.

Will search keywords be provided that optimize possibilities for re-use?
No.

Do you provide clear version numbers?
Yes. File versioning will be normally used.

What metadata will be created?
File properties.

WP 8- Dissemination and Exploitation

DPM Component	Issues to be addressed
Data Summary	What is the purpose of the data collection/generation in WP? What types and formats of data will the project generate/collect? Will you re-use any existing data and how? What is the origin of the data?

	What is the expected size of the data? To whom might it be useful ('data utility')? Are the data produced and/or used discoverable with metadata, identifiable and locatable by means of a standard identification mechanism (e.g. persistent and unique identifiers such as Digital Object Identifiers)? What naming conventions are followed? Will search keywords be provided that optimize possibilities for re-use? Do you provide clear version numbers? What metadata will be created?

What is the purpose of the data collection/generation in WP?

WP8 aims at the "Dissemination and exploitation" of the project results and combines the creation of content for the communication to the general audience and to specific groups with the collection of information about the potential interest by potential customers in the project outcomes.
In addition to that, it aims at building a community made of experts and stakeholders around the projects and to liaise with other similar initiatives and projects.
Finally, it targets standardisation.

What types and formats of data will the project generate/collect?

In Task 8.1 and Task 8.3 many initiatives to reach out to interested people are planned. They include workshops, the project website and Social Media.
The typical data sets (collected with permissions using forms) are:

- Full name, affiliation, email of participants to workshops and meetings
- Group (e.g. private industry, Public Authority…)
- Links to personal account to social media (if provided)
- Notes and minutes of the workshops and/or meetings
- Footage and recording of interviews

It is possible that authorisation to get filmed or photographed are requested to the participants.
For running the project website, cookies are needed.

Task 8.4 and Task 8.6 collect information on market and businesses, therefore, does not collect personal data apart from the contact information of the persons asked for providing those elements.
The typical data sets are:

- Full name, affiliation, email of contact persons
- Group (e.g. private industry, Public Authority…)
- Notes and minutes of the workshops and/or meetings

Task 8.2 and Task 8.5 do not foresee the collection of any data

All data are stored in .docx; .PDF; .XLSX format, with exception of the recording/footages, stored as .jpeg .mp3, .mp4 and other multimedia formats

Personal data collected will be anonymized, encrypted and sanitized by proper anonymization/pseudonymization techniques. All data that are restricted will be encrypted and password protected. The consortium agreed to adopt ZedPro software for the encryption of data.

What is the origin of the data?

For individuals, the persons themselves, using paper or digital forms
For the general public via the Internet, statistical information from Google and other third Parties

Will you re-use any existing data and how?

It is possible to use existing data, provided by associations and working groups.

What is the expected size of the data?

The size of the files ranges from 0.1-1 Mb for the textual ones to 1-100 Mb for multimedia files.

To whom might it be useful ('data utility')?

All partners involved in the project.

Potentially, data related to marketing and business may be useful to interested third parties for further studies, commercial initiatives and statistical analyses.

Are the data produced and/or used discoverable with metadata, identifiable and locatable by means of a standard identification mechanism (e.g. persistent and unique identifiers such as Digital Object Identifiers)?
No

What naming conventions are followed?
The file name must include the production date, the version and the partner that produced it. No specific convention for the description of the subject of the file.

Will search keywords be provided that optimize possibilities for re-use?
No

Do you provide clear version numbers?
Yes – all data are stored in files with versioning and production date.

What metadata will be created?
None (except the file property medatada).

WP9- Ethics

References

—. 2000. Qualifiers. [Online] 2000. https://www.dublincore.org/specifications/dublin-core/dcmes-qualifiers/

—. 2002. ISO/IEC 15938-1:2002, Information technology — Multimedia content description interface — Part 1: Systems. [Online] 2002. https://www.iso.org/standard/34228.html.

—. 2003. ISO/IEC TR 20943-1:2003, Information technology — Procedures for achieving metadata registry content consistency — Part 1: Data elements. [Online] 2003. https://www.iso.org/standard/34343.html

—. 2003a. ISO 19115:2003, Geographic information — Metadata. [Online] 2003a. https://www.iso.org/standard/26020.html

—. 2012. ISO 16684-1:2012, Graphic technology — Extensible metadata platform (XMP) specification — Part 1: Data model, serialization and core properties. [Online] 2012. https://www.iso.org/standard/57421.html

—. 2019. ISO/IEC 11179, Information Technology -- Metadata registries (MDR). [Online]

2019. http://metadata-standards.org/11179/

—. 2020. Type Vocabulary. [Online] 2020. https://dublincore.org/specifications/dublin-core/dcmi-terms/#section-7

DCMI. 1995. Dublin Core Metadata Initiative. [Online] 1995. https://www.dublincore.org/.

EU GDPR Website, GDPR portal: https://www.eugdpr.org/.

Data Management, Participant Portal H2020 Online Manual, Cross Cutting Issues and Data Management, http://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm

H2020 Programme, Guidelines on FAIR Data Management in Horizon 2020, Version 3.0, 26 July 2016, http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

H2020 Programme, Guidelines to the Rules on Open Access to Scientific Publications and Open Access to Research Data in Horizon 2020 Version 3.2, 21 March 2017, https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-pilot-guide_en.pdf

IANA. 2020. Media Types. [Online] 2020. https://www.iana.org/assignments/media-types/media-types.xhtml

IPTC. 2019. Information Interchange Model (IPTC) Photo Metadata Standard. [Online] 2019. https://iptc.org/standards/photo-metadata/iptc-standard/.

ISO. 2017. ISO 15836-1. *Information and documentation — The Dublin Core metadata element set — Part 1: Core elements.* [Online] 2017. https://www.iso.org/standard/71339.html.

Microsoft. 2018. Imagery Metadata. [Online] 2018. https://docs.microsoft.com/en-us/bingmaps/rest-services/imagery/imagery-metadata.

Milenkovic, Milan. 2015. A Case for Interoperable IoT Sensor Data and Meta-data Formats: The Internet of Things (Ubiquity symposium). [Online] 2015. https://doi.org/10.1145/2822643.

NISO. 2004. *Understanding metadata, National Information Standards.* 2004.

OMG. 2017. Meta-Modeling and the OMG Meta Object Facility (MOF). [Online] 2017. https://www.omg.org/ocup-2/documents/Meta-ModelingAndtheMOF.pdf

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). http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

W3C. 2012. Web Ontology Language (OWL). [Online] 2012. https://www.w3.org/OWL/

Wilkinson et al., “The FAIR Guiding Principles for scientific data management and stewardship”, 2016, Scientific Data 3:160018, https://doi.org/10.1038/sdata.2016.18