D1.2 – Project Data Management Plan PDMP

Editor(s): ED

Contributors: All Partners

Reviewed by: BDI, SATCEN

Quality Review by: ED

Official Submission Date: 2023-03-31

Actual Submission Date: 2023-03-31

Dissemination Level: Public

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101073985

Copyright notice - Disclaimer

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

Executive Summary

This deliverable constitutes the Data Management Plan (DMP) of the EURMARS project, outlining the main elements of the data management policy that will be used by the whole Consortium. The DMP gives a general outline of the rights and the integrity of all generated/processed/collected data as well as the procedures that will be followed to acquire the data with respect to their sensitivity and the measures that need to be followed throughout this process. In that way, the DMP presents how research data will be handled during the EURMARS project, and even after the project is completed, describes what data, methodology and standards will be followed, and whether this data will be shared and/or made open. Moreover, only public information has been provided in this document, thus for a more detailed understanding of specific procedures needed to handle specific data in the project, other documents have been provided in the context of EURMARS, such as a number of provisions on Ethical aspects fulfilling ethical requirements.

The present deliverable constitutes the Project Data Management Plan at Month 6 of the project. The described data management policy reflects the current state of Consortium agreements regarding data management and is consistent with those referring to the exploitation and protection of results and can also be considered as a checklist for the future. Moreover, the different aspects of making data Findable, Accessible, Interoperable, and Re-usable (FAIR) are presented.

Table of Contents

Table of Tables

List of Abbreviations

Term	Description
DMP	Data Management Plan
DoA	Description of Action
DOI	Digital Object Identifiers
DPO	Data Protection Officer
EC	European Commission
EUCI	European Union Classified Information
FAIR	Findable, Accessible, Interoperable, Re-usable
GDPR	General Data Protection Regulation
IPR	Intellectual Property Rights
WP	Work Package

1 Introduction

1.1 Overview

This deliverable aims to provide an extensive analysis of the main elements of the data management policy that will be used by the participants of the EURMARS project with regard to all the datasets that the project will generate. It describes the data management life cycle for all data sets that will be collected, processed, or generated by the EURMARS project. This deliverable presents how data will be handled during and even after the project is completed, describing:

- the data,
- implemented methodology and standards,
- data sharing and open access practices,
- data curation and preservation practices.

1.2 Structure of the deliverable

This deliverable aims to present the Data Management Plan of the EURMARS project. The structure of the document is as follows:

- Section 2 describes, among others, the purposes of data collection or generation, the types and formats of collected or generated data, data origin, expected data size, and access levels.
- Section 3 presents the FAIR (Findable Accessible Interoperable Reusable) principles that guide the project's data management.
- Section 4 describes the allocation of resources, including the costs of implementing the FAIR principles and how the costs will be covered throughout the whole period of the project.
- Section 5 outlines the provisions which are implemented for data security and safe storage (partners' repository or database) to preserve and curate the data.
- Section 6 outlines the ethical and legal aspects that may influence data sharing, including references to ethics deliverables and the ethics chapter in the Description of the Action (DoA).

- Section 7 describes the management of Intellectual Property Rights (IPR).
- Section 8 concludes this deliverable.

2 Data Summary

2.1 Purpose of the data collection/generation and relation to the objectives of EURMARS

Data collection, generation, and processing are integral for EURMARS to meet its objectives. The purpose is described as follows:

- Data exploited for research purposes in creating deliverables in almost all WPs through desktop research and literature review, interviews, and workshops in the form of recordings, written notes, and transcripts.
- Data exploited for research purposes in WP2 in the framework of identifying the end-user requirements, training scenarios, and the development of a comprehensive perspective on maritime border surveillance, situational awareness, and authorities' response mechanisms to different incidents, including an in-depth analysis of various social and organisational processes, work practices, user roles, and operational environments.
- Data regarding the integration in WP4.
- Data extracted from the pilot implementation and Living Labs in W5.

2.2 Types and formats of data that EURMARS will generate/collect

In order to fulfil the purpose of the data collection/generation, the EURMARS project will collect and generate the following types and formats of data:

Table 1. Types and formats of data

Data/Data Source	Data type	Data format	Data origin
Surveys, workshops/living labs	Electronic document	• Word document (.doc,.docx)	WP2, WP3, WP4, WP6, WP7

data, validation cycles data		• Excel document (.xls/.xlsx) • Pdf document	
	Hardcopy	paper	
Deliverables	Electronic document	• Word document (.doc,.docx) • Excel document (.xls/.xlsx) • Pdf document	All WPs
	Hardcopy	paper	
Website public reports	Electronic document	• Word document (.doc/.docx) • Pdf document • Excel document (.xls/.xlsx) • .csv files • .txt	All WPs
Video files	Electronic document	.mov, .mpeg, .avi, .mp4, etc.	All WPs
Audio files	Electronic document	.mp3, .wav, etc.	All WPs
Images	Electronic document	.jpg, .png, .gif, etc.	All WPs
Software	Source Code	Source Code	WP3, WP4
Signed documents (eg. Consent forms, information sheets, attendance lists, Consortium Agreement, etc.)	Electronic document	• Word document (.doc,.docx) • Excel document (.xls/.xlsx) • Pdf document	WP1, WP2, WP5, WP6
	Hardcopy	paper	
Presentations	Electronic document	Powerpoint document	All WPs
	Hardcopy	paper	
Network and system related data	Electronic data		WP3, WP4, WP5, WP6

2.3 Information types in the EURMARS project.

Following the "Guidance Guidelines for the classification of research results" of the European Commission, the deliverables have three types of classification: PUBLIC, SENSITIVE, and RESTREINT UE/EU RESTRICTED.

2.3.1 PUBLIC

In Table 2, EURMARS deliverables are classified as PUBLIC.

Table 2. Public deliverables

Number	Deliverable Title
D1.1	Project Quality Management Plan PQMP
D1.2	Project Data Management Plan PDM
D1.3	Ethics and Innovation Management
D2.4	AI Act Foresight Report and Blueprint, PIA, EIA and SIA assessment
D4.5	Integration and Test Reports
D5.4	Evaluation, Benchmarking and Lessons Learned
D6.1	Exploitation, Dissemination, Standardisation Report – 1st Release
D6.2	Exploitation, Dissemination, Standardisation Report – 2nd Release
D6.3	Exploitation, Dissemination, Standardisation Report – 3rd Release
D6.4	Stakeholders Engagement and Industrial Showcase

2.3.2 SENSITIVE

In Table 3, EURMARS deliverables are classified as SENSITIVE.

Table 3. Sensitive deliverables

Number	Deliverable Title
D2.1	Requirements and Assessment Methodology
D2.2	EURMARS System Architecture - 1st Release
D2.3	EURMARS System Architecture – 2nd Release
D7.1	H - Requirement No. 1
D7.2	H - Requirement No. 2
D7.3	POPD - Requirement No. 3
D7.4	AI - Requirement No. 4

2.3.3 Classified Information: RESTREINT UE/EU RESTRICTED (Commission Decision 2015/444/EC)

In Table 4, EURMARS deliverables are classified as RESTREINT UE/RESTRICTED EU.

Table 4. EU-R deliverables

Number	Deliverable Title
D3.1	Sensor Development – 1st Release
D3.2	Sensor Development – 2nd Release
D3.3	Interfaces to External IT Services - 1st Release
D3.4	Interfaces to External IT Services – 2nd Release
D3.5	Sensor Fusion Software Module - 1st Release

D3.6	Sensor Fusion Software Module -2nd Release
D4.1	Collaborative C2 including subsystems, Visualization & Alarming - 1st Release
D4.2	Collaborative C2 including subsystems, Visualization & Alarming -2nd Release
D4.3	Risk Assessment Framework & Decision Support - 1st Release
D4.4	Risk Assessment Framework & Decision Support -2nd Release
D5.1	Pilots Definition
D5.2	Test Report from Demonstrations - 1st Release
D5.3	Test Report from Demonstrations – 2nd Release

2.4 Origin of the data, reuse of existing ones and expected size of the data

To support the project deliverables, data will be collected, evaluated, and aggregated from end-users and external stakeholders engaged in the project activities, acquired through desktop research, Living labs, workshops and surveys. Potential existing data will be exploited in the form of published materials relating to maritime and border security and serve as a reference in order to analyse operational or other incidents that may occur.

To support the development of the EURMARS components, data from various sensors (cameras, satellites, etc) will be used.

The expected size of the data collected/generated/processed under the EURMARS project ranges from kilobytes to gigabytes, even terabytes, depending on the period of retention of the data, the sensor data, and the transcripts of the surveys/living labs.

3 FAIR data

FAIR (Findable Accessible Interoperable Reusable) principles provide guidelines for better data management and making the data accessible, interoperable, and reusable. In the following, the approach of the EURMARS project to each FAIR principle is addressed within dedicated sub-sections.

3.1 Making data findable, including provisions for metadata

EURMARS project complies with the principal priorities as defined below:

- The publications will be made available through the project's website, and the data produced will be discoverable with metadata and identifiable and locatable by the Digital Object Identifiers (DOIs). The metadata will include: title, data types/formats and software, data collection method and dates, geographic coverage, language, data processing details, funding details, ethics clearance details, a project abstract, keywords, and licensing.
- Data needed for the collaborative tools are expected to include a unique ID and a timestamp allowing for proper indexing and handling when stored. No specific standards or metadata have been identified for the time being for the datasets.
- The data from the surveys, workshops/living labs, and the validation cycles will not be published as primary data (data that is collected directly from the data source) due to privacy and security concerns.

3.2 Making data openly accessible

All publications will be made available through ArXiv (https://arxiv.org/) repository or OpenAIRE (https://www.openaire.eu/).

Additionally, the interview data (recordings, protocols, and transcriptions) from experts will not be made openly available and will not be published as primary data due to privacy and security concerns. Anonymization is not considered as an alternative, because the limited number of the interviews allows for drawing conclusions on the respondents. The anonymous results could be used for publishing academic papers on maritime and border security training needs.

The dataset obtained under WP3, WP4, and WP5 might contain classified information related to the existing mechanisms/processes/infrastructure used for maritime and border security, hence these datasets will be classified.

3.2.1 Data produced or collected made accessible

Access to the data will be controlled through strict and secure authentication and authorization services, supported by role-based access control, thus ensuring that only authenticated and authorized users can access the stored information.

The data from the surveys will not be accessible by all consortium partners as primary data due to privacy and security concerns.

3.3 Making data interoperable

The concept of interoperability demands that both data and metadata must be machine-readable and that a consistent terminology is used. To that extent, a specific document template (xml, json, etc) describing the structure of the exchanged information will be used.

3.3.1 Standard vocabulary

In almost all cases, the vocabulary used will be standard for all data types and make use of a common language within the business creation culture. Vocabulary won't represent any barrier to data interoperability and re-use.

3.4 Increase data re-use

The re-use of data (if needed) will be restricted to the research use of the license and anonymous data can be used for scientific publications. Data may not be copied or distributed and must be referenced if used in publications. The collected data will be a consolidation of data from several sources, each one having its own policies.

Use of Creative Commons licenses, the default being CC-BY 4.0, which makes data very widely re-usable shall be encouraged for research articles, allowing copying, distribution, and transmission of work without affecting essential author rights.

4 Allocation of resources

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

In general, the person responsible for data management and compliance regarding the EURMARS project is the Data Protection Officer (DPO), as well as the contact point and DPOs of each organisation.

5 Data Security

The data collected/generated throughout the whole period of the EURMARS project will be held in data repositories in the servers of organisations. The servers will be kept in locked rooms with authorized access and will adhere to appropriate security standards as well as to state-of-the art security mechanisms. The data repositories will be accessed by authorized personnel both at physical and network levels. The databases will have a dedicated identification and authentication mechanism, name and password, for each authorized user and will adhere to different access privileges for the authorized users of the organisation in any case.

Access to the data repository will be achieved through the appropriate protocols. The transfer of the data (e.g. files, deliverables, raw data etc.) will be achieved using encryption methods (e.g. file transfers, encrypted disks, encryption keys, a physically protected and secure PC responsible for this process) when necessary.

As for the "physical" data storage, the documents will be kept in an office's secure environment, in computers with authentication and authorization mechanisms. If there are documents with restricted access, they will remain in a locked cabinet at the organisation's premises.

Backups of the databases will be stored encrypted and on the organisations' premises. Data backups of devices will happen every week and be stored in devices that follow the same security standards and procedures as the main server.

6 Legal framework and guidelines

Applicable legislation on the protection of personal data:

- Regulation (EU) 2016/6792 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).
- Regulation (EU) 2018/17253 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/20014 and Decision No 1247/2002/EC5.
- National data protection laws.

Applicable legislation on the protection of EU classified information:

- Commission Decision (EU, Euratom) 2015/4446 of 13 March 2015 on the security rules for protecting EU classified information.
- Directive (EU) 2016/11487 of the European Parliament and of the Council of 6 July 2016 concerning measures for high common level of security of network and information systems across the Union.

6.1 Personal Data Management

6.1.1 Important GDPR provisions

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

According to Recital 26 GDPR, the principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no

longer identifiable. Since GDPR does not apply to anonymous information, it is very important to distinguish between anonymised and pseudonymised data, as for the latter GDPR remains applicable.

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

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

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

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

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

of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.

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

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

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

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

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

6.1.2 Handling of personal data in the EURMARS Project

With respect to all data processing activities of the Project as they are described above in detail, constant guidance will be provided by the Ethics Board Members designated for the EURMARS Project, the Data Protection Officer appointed for the Project, and the Data Protection Officer of each partner as listed in D7.3 POPD-Requirement No.3. For partners not having appointed a DPO, a data protection policy exists which is also included in D7.3 POPD-Requirement No.3.

The EURMARS Consortium commits to the protection of personal data processed during the lifetime of the research project and will implement the appropriate safeguards in order to be compliant with

the GDPR provisions. All partners respect the principle of data minimization. Technical and organisational measures, as well as security measures that are/will be implemented by each EURMARS partner are described in D7.3 POPD-Requirement No.3.

6.2 Handling of EU Classified Information

The EURMARS Consortium is obliged to respect the security rules for protecting EU Classified Information (EUCI), as laid down in Commission Decision (EU, Euratom) 2015/444. This means that the EURMARS partners will handle EUCI in line with the principles, rules and procedures established therein. By compromising or losing EUCI we are aware that we not only breach the grant agreement, we are also liable to disciplinary and/or legal action per applicable (national) laws, rules and regulations. In EURMARS, the deliverables marked as RESTREINT UE/EU RESTRICTED have been presented in Section 2.3.3.

For information marked as such no Personnel Security Clearance Certificates need to be issued according to the aforementioned Euratom Decision.

However, the EURMARS Consortium is aware that RESTREINT UE/EU RESTRICTED deliverables require special treatment.

- Need-to-know: To access EUCI, individuals need to have a need-to-know (i.e. you need the information to perform a specific professional function or task).
- Awareness of the Security Rules: Individuals may only be granted access after they have been briefed on the security rules and have acknowledged their responsibilities.
- By post: Documents should be sent in double, opaque envelopes. The inner envelope must be sealed and marked RESTREINT UE/EU RESTRICTED. The documents/USB keys/CD roms must be placed into the inner envelope and must bear the same marking.
- Electronic transmission: The documents are encrypted with approved encryption tools (i.e. FILKRYPTO) and sent via e-mail. EU classified deliverables shall not be uploaded via the portal.
- Storage: When not in use, the documents shall be stored in a locked container or a locked cupboard.
- Consultation: Only in secure areas where nobody is able to read or remove the documents.
- Printing/copying: Printing and/or copying of the documents is not allowed.

- Notes: Reference to EUCI in the partners' notes means that the notes should be treated as RESTREINT UE/EU RESTRICTED documents.

- Communication: There shall be no communication about the EUCI via phone, e-mail or in unsecured areas. The information shall not be discussed with persons who do not have a justified need-to-know.

- Meetings: Meetings on EUCI are organised on an invitation-only-basis and all attendees need to have a need-to-know. Attendees should sign an attendance sheet at the beginning of a meeting. Meetings should take place behind closed doors. The windows and blinds in the room must be closed. Mobile phones and other portable devices must be switched off or left outside of the meeting room. Wireless microphones may not be used and microphones/speakers should be switched off. If RESTREINT UE/EU RESTRICTED documents are distributed at the beginning of a meeting, the exact number of documents necessary must be distributed and they must be returned to the Chair, collected and accounted for. No stock may be held in the room. If EUCI is presented or projected on a screen, the computer or laptop used must not be connected to a network. During breaks, meeting rooms must be locked and guarded. Feedback on EUCI must be raised during the specific time slot dedicated to its discussion (on the agenda).

- Breach or compromise: In case of a (potential) breach or compromise of EUCI, the partner/partners must immediately inform the REA SPOC TEAM (REA EUCI SPOC <REA-EUCISPOC@ec.europa.eu>) and the responsible REA Project Officer. No attachment of EU Classified Information shall occur during this communication.

- Duration: Obligations vis-à-vis the protection of EU classified information continue to persist after the life of the project.

7 Intellectual Property Rights (IPR) Management

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

7.1 Definitions

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

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

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

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

7.1.1 Applicable legislation

- European Patent Convention, 16th edition9 (published June 2016) which contains the Convention on the Grant of European Patents (EPC) as in force since 13 December 2007, the EPC Implementing Regulations as in force since 1 May 2016 but also including an amendment that entered into force on 1 November 2016, the rules of procedure of the EPO boards of appeal and Enlarged Board of Appeal, included for the first time in an edition of the EPC, the

protocols forming integral parts of the EPC (Protocol on the Interpretation of Article 69 EPC, Protocol on Centralisation, Protocol on Recognition, Protocol on Privileges and Immunities, Protocol on the Staff Complement), an extract from the EPC Revision Act of 29 November 2000, the Administrative Council's decision of 28 June 2001 on the transitional provisions under Article 7 of the Revision Act, and the Rules relating to Fees.

- Regulation (EU) 2017/100110 of the European Parliament and of the Council of 14 June 2017 on the European Union trademark.
- Council Regulation (EC) No 6/200211 of 12 December 2001 on Community designs.
- Directive (EU) 2019/79012 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Directive on Copyright in the Digital Single Market).
- Directive 2001/29/EC13 of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.
- Directive 96/9/EC14 of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.
- Directive 2009/24/EC15 of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs.
- Directive 2004/48/EC16 of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.
- National laws on patent, design, trademark and copyright protection.

7.2 IPR Management in the EURMARS Project

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

In particular, Section 8 Results and Section 9 Access Rights of the EURMARS Consortium Agreement include all relevant clauses that have been agreed between the partners and refer to the IPR management. In Attachment 1 of the EURMARS Consortium Agreement, the Parties have identified and agreed on the Background for the Project and have also, where relevant, informed each other

that access to specific Background is subject to legal restrictions or limits. Therefore, we aim to work methodically in order to classify EURMARS IPRs and define:

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

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

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

To effectively achieve the aforementioned objectives regarding the overall management of IPRs, a cumulative IPR Control form will be circulated by the coordinator.

8 Ethical Aspects

Work package 7 (Deliverables 7.1, 7.2, 7.3 and 7.4) of the EURMARS project deals with the ethics requirements with which EURMARS's objectives, methods, processes, tasks and results must comply. These ethics requirements mainly relate to the processing of personal data and, with that, with data protection. Therefore, in this deliverable, requirements that deal specifically with the procedures with respect to data protection will not be covered.

In order to ensure that all ethical aspects are considered and that the EURMARS project is compliant with all legal requirements and ethical issues, a general strategy has been designed based on the Ethics Requirements that were defined by deliverables from WP7. This strategy involves an ad hoc monitoring process of the project development by applying the privacy-by-design approach through a methodological design based on a "Socio-legal Approach." This is a risk-based approach to privacy and data protection issues in line with the new General Regulation for Data Protection (GDPR).

Ethics Requirements that were drawn by the EC, during the ethics check process before the signature of the GA, have been taken into account by the consortium; to address all these requirements the EUMRARS beneficiary Trilateral Research Limited, with its ethical and legal expertise will provide general guidelines to the project and the consortium on all aspects, covering data protection, privacy issues, research participants' safety, etc.

9 Conclusions

The present deliverable constitutes the Project Data Management Plan at Month 6 of the project. As such, the present deliverable must be intended as a guideline with respect to data management, reporting the main principles that EURMARS project is adherent to and providing a snapshot on the implications of Security and Ethics on data management.

Moreover, only public information has been provided in this document, thus for a more detailed understanding on specific procedures needed to handle specific data in the project, other documents have been provided in the context of EUMARS, such as a number of provisions on Ethical aspects fulfilling ethical requirements.

EURMARS

An advanced surveillance platform to improve the EURopean Multi Authority BordeR Security efficiency and cooperation