HISEA DELIVERABLE 7.4

REPORT ON THE ETHICS REQUIREMENTS RELATED TO COLLECTION, STORAGE AND PROCESSING OF PERSONAL DATA

WORK PACKAGE NUMBER: 7

WORK PACKAGE TITLE: INNOVATION MANAGEMENT, EXPLOITATION AND BUSINESS PLANNING

HISea Project Information	
Project full title	High Resolution Copernicus-Based Information Services at Sea for Ports and Aquaculture
Project acronym	HiSea
Grant agreement number	821934
Project coordinator	Dr. Ghada El Serafy
Project start date and duration	1st January 2019, 30 months
Project website	https://hiseaproject.com/

Deliverable Information	
Work package number	7
Work package title	Innovation Management, Exploitation and Business Planning
Deliverable number	7.4
Deliverable title	Report on the ethics requirements related to collection, storage and processing of personal data
Description	This deliverable will address the requirements related to collection, storage and processing of personal data. The document will include the main issues (e.g. obtaining ethical approvals for the collection of personal data by the competent National Data Protection authority) that need to be taken into account by the partners when dealing with the data protection and privacy aspects. This document will also provide guidance for the identification of the privacy and data protection aspects and how such issues need to be dealt with in the project along with a description of the measures that need to be taken in order to comply with the relevant EU rules.
Lead beneficiary	Ascora
Lead Author(s)	Danny Pape

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 821934

Contributor(s)	Bracha Ehrman
Revision number	3
Revision Date	31/10/2019
Status (Final (F), Draft (D), Revised Draft (RV))	Final
Dissemination level (Public (PU), Restricted to other program participants (PP), Restricted to a group specified by the consortium (RE), Confidential for consortium members only (CO))	PU

Document History			
Revision	**Date**	**Modification**	**Author**
0.1	02/09/2019	create structure, edit content	Danny Pape
0.2	22/10/2019	Review, edit	Bracha Ehrman
0.3	30/10/2019	Address comments and review editing, edit	Adi Shoval Danny Pape
0.4	30/10/2019	Review	Sandra Gaytan

Approvals				
	Name	**Organisation**	**Date**	**Signature (initials)**
Coordinator	Dr. Ghada El Serafy	Deltares	31/10/2019	GS
WP Leaders	Simon van Dam	Agora	31/10/2019	SvD

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 821934

Executive Summary

This document highlights the main ethical issues arising during the development and research phases, especially with regards to the involvement of end-users in the design and use of the HiSea Platform. HiSea will require access to the user's personal data and tracking of their data searches to optimise and accelerate other model requests. Recommendations to ensure data protection and privacy from a regulatory and ethical perspective are provided within a guideline for developers.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 821934

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 821934

1 Introduction

The HiSea project is developing advanced data services tailored to its users' needs. The services are enabled by a platform developed in the project which can provide these services through knowledge generated by data retrieved from the COPERNICUS system. The greatest asset of an online platform is its users. Therefore, it is very important to protect the personal data of the users at all times and, in case of a breach in protection, to handle the situation transparently.

However, this also represents a great responsibility, particularly in the safeguarding of personal data. There are different critical stages where personal information is managed. Some examples include the registration step, and the creation of a hierarchy of roles and users for controlling the access to restricted resources in the platform.

Deliverable 7.4 Report on the ethics requirements related to the collection, storage and processing of personal data, is aimed primarily at project developers and describes the specific requirements that will guide their work while developing the HiSea platform.

This deliverable is broken down into the following sections:

Section 2: Scope of the relevant data protection regulation

Section 3: Impact of the regulation on HiSea

Section 4: Conclusions

2 Scope

In order to define the scope of ethical issues which must be addressed by the HiSea project, the following subsections provide a brief overview of the common but often misleading terminology as well as information about non-EU partners and the General Data Protection Regulation 2016/679 ("GDPR").

2.1 Definitions

Privacy

Westin defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" [We67].

The scope and consent of what is considered to be "private" differ among cultures and individuals but share basic common themes. Privacy may, therefore, include anonymity, the wish to be unidentified in some cases. When an element within an IT-system such as HiSea is referred to as being "private", it usually means that it may be considered as being especially important or sensitive on a personal level to the individual. The degree to which private information is exposed therefore depends on how the public will receive this information, which differs from place to place and over time. Privacy may intersect with

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 821934

security aspects, including, e.g., the concepts of appropriate use, as well as protection of information. Almost all countries have laws which in some way limit privacy.

The importance of privacy has been highlighted by the on-going discussions about PRISM and Tempora (NSA surveillance scandal, June 2013), and the large impact this issue has on society and the digital sector even a few years later, have been revealed. The broad absence of privacy in this domain and the discussion connected to it, have shown the need for IT systems to respect privacy in order to form a base for a trusty environment.

Personal Data

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 Article 4(1) of GDPR (Regulation (EU) 2016/679).

Processing

'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction according to Article 4(1) of GDPR (Regulation (EU) 2016/679).

Data Privacy

The term privacy may be used for different things in different contexts. Different people, cultures, and nations have a wide variety of expectations about what privacy covers or what causes an invasion of privacy. The most relevant aspect of privacy protection for HiSea is data privacy. Data privacy in HiSea needs to handle the trade-off between sharing data that is necessary for allowing HiSea to provide its services and protecting user-specific data from being shared unnecessarily. As such the challenge is to share data on the one hand while protecting personally identifiable information on the other hand

The ability to control the information one reveals about oneself via the Internet, and who can access that information, has become a growing concern and as such, it needs to be addressed by HiSea.

In order to not hinder the functionality of HiSea by processing personal data subjecting it to extensive privacy protection obligations, a good balance needs to be found. For example, by anonymizing all user personal data.and company-specific data before it leaves the client. This may allow users to provide more personal data without subjecting HiSea to extensive data protection duties that may affect the operability of the platform.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 821934

2.2 Involvement of non-EU countries

If any personal data is transferred from the EU to a non-EU country or international organization during the implementation of the project a confirmation that a personal data transfer is in accordance with Chapter V of the General Data Protection Regulation 2016/679 will be submitted to EC. In that case, it may be necessary to make a data transfer agreement with the recipient or obtain a specific authorization by the national data protection authority. In addition, in cases where personal data is transferred from a non-EU country to the EU (or to another third country), a confirmation that such a transfer complies with the legislation of the country in which the data was collected will be submitted. Finally, in case an activity undertaken in non-EU countries raises an Ethics issue, the HiSea project will ensure that the research conducted outside the EU is in line with the relevant and applicable EU legislation.

2.3 General Data Protection Regulation

The General Data Protection Regulation (GDPR) is a regulation on data protection and privacy for all individual citizens of the EU. It was introduced in April 2016 and became mandatory and enforceable on 25th May 2018. The goal of this regulation is to provide control to individuals over their own personal data so that they know what kind of personal data is saved, how it is used, and in certain circumstances require their consent for the processing of their data.

Clearly, Hisea platform development is affected by the above-mentioned privacy issue and as such developers must follow the requirements of this regulation. The table below details some of the main requirements and their specific relevance for HiSea, including the likelihood of occurrence and measures that will be taken by HiSea to comply with each requirement.

GDPR Requirements	**HiSea Relevance (level of likelihood and measures to be taken)**
Scope: The regulation applies to (1) the processing of personal data in the context of the activities of the data controller or processor (e.g. cloud service provider, such as DIAS) that), or the data subject (person) is established in the EU; or (2) to the processing of personal data of data subjects in the EU, by a controller or processor not established in the EU, where the processing activities relate to: (a) the offering of goods and services to such data subjects in the EU, or (b) the monitoring of their behaviour as it takes place in the EU; or (3) where the processing is performed by a	High. HiSea is designed specifically for the European market and will process the personal data and monitor the behaviour of data subjects in the EU in the course of offering its services and is thus subject to the GDPR.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 821934

controller not established in the EU, but in a place where Member State law applies.	
Accountability: the GDPR requires controllers to be responsible for, and able to demonstrate compliance with its core principles, including data minimization; lawfulness, fairness and transparency of processing activities; purpose limitation; accuracy, storage limitation, and integrity and confidentiality.	*High.* HiSea will process personal data only in accordance with such principles, and will implement procedures and other measures to ensure and to be able to demonstrate compliance with the GDPR.
Lawfulness of Processing: according to Article 6 of GDPR the processing of personal data must rely on one of the legal bases for processing detailed in Article 6 of the GDPR.	Medium. HiSea will ensure the processing of personal data is based on a legal basis in accordance with the GDPR, and will obtain the data subjects' consent where required.
Data Protection Officer: The GDPR requires the appointment of a Data Protection Officer ("DPO") where: (a) the processing is carried out by a public authority or body; (b) the core activities of the controller or processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or processor consist of processing on a large scale of special categories of data.	Medium. The HiSea consortium will establish effective ethical management, rooted in the project, with a thorough understanding of both the underlying science as well as the associated ethical principles.
Data Protection by Design and by Default: The GDPR requires controllers to implement appropriate technical and organisational measures, such as pseudonymisation, designed to implement data protection principles and for ensuring that, by default, only personal data which are necessary for each specific purpose of processing are processed.	Medium. HiSea will implement technical and organisational measures to ensure data minimization and compliance with other data protection principles. For example: HiSea will ensure that the personal data collected on the HiSea platform will not be attributed to a specific person.
Data Breach Notification: According to the GDPR, in the case of a personal data breach, the controller is required to notify the competent supervisory authority of the breach without undue delay, and within no later than 72 hours of becoming aware of it. Where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the	Medium. HiSea will implement measures and procedures for the prevention, detection and notification of personal data breaches as required by the GDPRdata breach is detected and the individuals in the case that a negative impact on that person is determined.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 821934

controller shall communicate the data breach to the data subjects without undue delay.	
Data Subjects' Rights: The GDPR requires allowing data subjects to exercise their rights to rectification, erasure, restriction of processing, data portability, right to object, and right to not be subject to automated processing.	Medium. HiSea will create procedures and implement measures to allow data subjects to exercise their rights where applicable by the GDPR.
Records of processing Activities: The GDPR requires controllers to maintain records of its processing activities that include the information detailed in Article 30, and that shall be made available to the supervisory authority on request.	*Medium* HiSea will implement procedures and measures to record its processing activities that will include a permanent logging service.
Providing notice to the data subject before or at the time of collection: The GDPR requires controllers to notify the data subjects, at the time when personal data are obtained, with information such as: (a) the identity and contact details of the controller and its representatives; (b) the contact details of the DPO, where applicable; (c) the purpose and legal basis for processing the personal data, including the legitimate interest pursued by the controller as a basis for processing, where applicable; (d) any third parties who will have access to the personal data; (e) whether the controller intends to transfer the data to any country out of the EU and the safeguards taken by the controller for such transfer; (f) the retention period for the personal data processed by the controller; (g) the existence of data subjects' rights and how to exercise them; and (h) data subjects' right to lodge a complaint with the competent supervisory authority.	*High.* HiSea will compose a privacy policy that will contain all the required information as per Article 13 of the GDPR and will take measures to ensure that data subjects are exposed to it on or before any personal data is collected.

3 Impact to HiSea

Currently the world is facing the age of information where huge amounts of unnecessary information is collected and continually generated. Information is now an integral part of HiSea's services and activities and the project is therefore required to ensure compliance with the applicable privacy and data protection

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 821934

laws and regulations. for that purpose. HiSea introduces ethical guidelines for developers in order to fulfil this need.

Collection

The collection of data is the active process by a system of gathering personal data in order to store and process it at later stages. Data collection on the HiSea project will follow the guidelines below:

- Data must be relevant and not excessive in relation to the purpose for which they are processed.
- Data must be collected for explicit and legitimate purposes and used accordingly.
- When personal data is collected, the least intrusive and costly data collection method should be chosen.
- Confirmation of informed consent shall be obtained, where necessary.

Data Storage

The data storage of personal information is necessary to maintain users' personal data for the necessary retention period in accordance with the purpose of processing. In order to avoid storage of unnecessary information, the following guidelines should be observed:

- Data must be accurate and updated as necessary.
- Data that identifies individuals must not be kept longer than necessary, considering, among others, the purpose for the collection and processing of such data.

Processing

- Data must be processed fairly and lawfully.
- Data controllers are required to provide reasonable measures for data subjects to exercise their rights with regards to their personal data.

General

Certain aspects should be considered in all processes throughout the chain of transferring data. These include:

- **Anonymisation** is the process used to strip personal data from all elements likely to help identify directly or indirectly the data subject (e.g. name, age, address, social security number, etc.). These elements are deleted to ensure re-identification is not possible.
- **Pseudonymisation** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 821934

subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

- **Encryption** is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption doesn't prevent hacking, but it reduces the likelihood that the hacker will be able to read the data that is encrypted.

4 Conclusion

This deliverable describes some of the main obligations that apply to the HiSea project with regards to its data collection and processing activities. It details some of the most important GDPR issues and their relevance to the HiSea project, but not all. All issues should be addressed on a rolling basis throughout the duration of the project. Likewise, the involvement of non-EU countries shall be considered, especially considering that the consortium partner- Agora is based in Israel.

5 References

[We67] Westin, A.: Privacy and Freedom, Atheneum, 1967

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 821934