PROJECT DELIVERABLE REPORT

NAIADES

Greening the economy in line with the sustainable development goals

D1.4 NAIADES Data Collection & Ethical Plan

A holistic water ecosystem for digitisation of urban water sector

SC5-11-2018

Digital solutions for water: linking the physical and digital world for water solutions

"This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 820985"

Document Information

Grant Agreement Number	820985	Acronym	NAIADES
Full Title	A holistic water ecosystem for digitization of urban water sector		
Topic	SC5-11-2018: Digital solutions for water: linking the physical and digital world for water solutions		
Funding scheme	RIA - Research and Innovation action		
Start Date	1stJUNE 2019	**Duration**	36 months
Project URL	www.naiades-project.eu		
EU Project Officer	Alexandre VACHER		
Project Coordinator	CENTER FOR RESEARCH AND TECHNOLOGY HELLAS - CERTH		
Deliverable	D1.4 NAIADES Data Collection & Ethical Plan		
Work Package	WP1– Project management, Quality Assurance and reporting		
Date of Delivery	**Contractual** M9	**Actual**	M9
Nature	R - Report	**Dissemination Level**	PU-PUBLIC
Lead Beneficiary	VUB		
Responsible Author	Vagelis Papakonstantinou Dimitra Markopoulou	Email	vagelis@papakonstantinou.me Dimitra.Markopoulou@vub.be
		Phone	
Reviewer(s):	EURECAT, ADSYS		
Keywords	Processing of personal data, ethical principles		

Revision History

Version	Date	Responsible	Description/Remarks/Reason for changes
0.1	15/02/2020	VUB	Report write-up
0.2	20/02/2020	EURECAT, ADSYS	Inclusion of partners' contributions
0.3	21/02/2020	VUB	Internal Review
1.0	28/02/2020	VUB	Review and Release
1.1	May 2021	VUB	Review of rejected deliverable after project's interim review meeting. Amendments in the following Chapters: 4.1.(a): Clarified that "NAIADES will apply on large datasets from water utilities in three European countries", instead of "NAIADES will apply on diverse big data that is collected by such water monitoring and control systems" 4.1.(b): Removed the "microsystems / micro-, nano- sensors" 4.1.(b): Inserted the last paragraph (p.17) to address the reviewers' comment *"Please clarify how the decision of going for the development of a Global Water Observatory, instead of predictive AI analytics for consumer confidence, downsized the need for the Ethics structure and to which extent the data gathered by the Consortium are still ethically relevant".* In addition, the reviewers' findings on "the deliverable number in the footnote is wrong (D1.), the table is incomplete (who is in charge for the final review/date)" have been addressed.
1.5	June 2021	EURECAT, ADSYS	Internal review of amended report
2.0	June 2021	VUB	Review and Release

Contents

1 Summary 1
2 Personal data protection under the EU Regulatory framework and in particular Regulation 2016/679 (GDPR) 2
2.1 EU regulatory framework 2
2.2 Main definitions under the GDPR 2
2.3 Principles relating to personal data processing under the GDPR 5
2.4 The lawfulness of processing in particular 6
2.5 What is considered valid consent under the GDPR 6
2.6 Processing of personal data in research 7
2.7 Rights afforded to individuals (data subjects) under the GDPR 9
2.8 Security of personal data 11
3 Ethics in research 1
3.1 How to conduct research ethically: Setting the regulatory landscape\ 1
3.2 List of ethical issues that may be encountered during research 3
3.2.1 Informed consent 3
3.2.2 Privacy / confidentiality 8
3.2.3 Vulnerable subjects 9
3.2.4 Civil application and dual use 11
3.2.5 Protection of personal data 12
3.2.6 Potential misuse of research findings 13
3.2.7 Information security 14
4 The NAIADES project: ethical and legal compliance 16
4.1 Project's description 16
4.2 The project's particularities 18
4.3 NAIADES and ethics: compliance with ethical principles 18
4.3.1 The European Commission's checklist 18
4.3.2 List of ethical issues in the NAIADES project 19
4.4 NAIADES and the protection of personal data; Compliance with the GDPR 23
4.4.1 NAIADES pilots 23
4.4.2 The NAIADES app 24
4.4.3 Security of processing in the context of the NAIDES project 24

4.4.4 The NAIADES app and data protection by design and by default 26
5 Conclusion 29
6 References 30

1 Summary

Purpose of this report is to evaluate the project's compliance with basic legal and ethical principles. The NAIADES research aims to introduce an innovative water management solution that will be validated through real life demonstrations in three different water management infrastructures. At the same time the project will focus on the design and implementation of the NAIADES framework. which is a personalised water behavioural change application, accessible via smartphones and tablets, which will enhance public awareness on water consumption and nudge behavioural water.

Given the project's description and particularities, it must be made sure that, both the research and the final solution, comply with ethical principles, such as the principle of privacy and confidentiality, of informed consent, of security of information and that it will respect the rights and freedoms of the people that may participate in it. Most importantly this report shall identify any personal data protection issues that may arise during the project execution and shall suggest measures the partners may implement for the NAIADES application to be designed with a focus on the protection of personal data.

The report is divided in three chapters. In the first chapter, EU personal data protection law is analysed, whereas the second chapter focuses on the ethical principles that apply to the project. Findings of the first two Chapters of this report are made concrete onto actual NAIADES circumstances in Chapter 3.

It is the report's ultimate purpose to provide the partners with helpful guidelines in order for them to stay in line with legal and ethical principles while running the project. In addition, it is anticipated that the present analysis will contribute to the partners' effort to design the NAIADES application with the data protection by design and by default principle in mind.

2 Personal data protection under the EU Regulatory framework and in particular Regulation 2016/679 (GDPR)

2.1 EU regulatory framework

Personal data protection has been in the centre of legislative efforts, at Member States level, since the 70's and at EU level since the 90's. The first regulatory instrument that was adopted at EU level was Directive 95/46/EC. The Data Protection Directive proved to be a useful tool in terms of protecting natural persons against unlawful processing of their personal data. However, as data processing methods became more invasive and rapid technological developments brought new challenges for the protection of personal data, the need for a more holistic solution became apparent. Therefore, in May 2016 the Directive was replaced by the General Data Protection Regulation (GDPR), which became fully enforceable in the European Union in May 2018. Contrary to the Directive, the GDPR is a regulatory tool of catholic and direct effect that intends to address any inconsistency in national laws and to warrant a harmonised personal data protection approach among Member States.

The GDPR regulates the processing by an individual, a company or an organization of personal data relating to individuals in the EU. The Regulation does not apply to the processing of personal data of deceased persons or of legal entities. Its provisions do not apply to data processing by an individual for purely personal reasons or for activities carried out in one's home provided there is no connection to a professional or commercial activity.

At the same time the protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

2.2 Main definitions under the GDPR

a) Personal Data

The definition of "personal data" is included in Article 4(1) of the 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.

The notion of identifiability is further addressed under recital 26 of the Regulation which reads as follows: "To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments". The recital clarifies that personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person.

The GDPR does not apply to anonymous information, that is information which does not relate to an identified or identifiable natural person. The same rule governs any data that were rendered anonymous in such a manner that the data subject is not or no longer identifiable.

b) "Processing" of personal data

A definition of "processing" of personal data is provided under Article 4(2) of the Regulation. Processing therefore 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".

c) Special categories of personal data and their processing

Special attention should be given to categories of data that do not fall under the generic definition of personal data mentioned above but to a specific group that of special categories of data. It is mentioned that the term sensitive data that was used in the Directive, is replaced in the Regulation by the term "special categories of personal data". These include:

- data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership
- genetic data that include personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
- biometric data that include personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data; and
- data concerning health that refer to personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status. The first two categories constitute additions in the data protection field that come as a result of scientific developments in their respective fields.

Article 9 (1) of the GDPR introduces a general prohibition as regards this category of data. The Article reads as follows: "processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited".

There are exceptions though to this general rule that are included in par. 2 of the same Article 9, and are outlined below:

a. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

b. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant

to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

c. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

e. processing relates to personal data which are manifestly made public by the data subject;

f. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

h. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

i. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

j. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

The last case (j) of article 9 is thoroughly examined below under 2.6 on the grounds of it being applicable to the NAIADES project, as a Horizon 2020 research project.

d) Controllers – processors – joint controllers – recipients

The definition of a **controller** is provided under article 4(7) of the GDPR. According to said provision controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law". New addition introduced by the Regulation is the explicit reference to the notion of joint controllers. Article 26 of the Regulation states that "Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation […]".

Article 4(8) defines a **processor** as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".

Finally, a **recipient** is defined under article 4(9). In particular, "recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not".

2.3 Principles relating to personal data processing under the GDPR

Principles relating to processing of personal data are included in article 5 of the GDPR. The article reads as follows:

1. Personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

To sum up, the processing principles provided under the General Data Protection Regulation are the principles of:

- **lawfulness, fairness and transparency**
- **purpose limitation**
- **data minimisation**
- **accuracy:**
- **storage limitation**

- **integrity and confidentiality**
- **accountability**

2.4 The lawfulness of processing in particular

Article 6 of the GDPR mentions the conditions that need to be observed in order for processing of personal data to be lawful. In short, these include:

-consent,

-performance of a contract,

-compliance with a legal obligation,

-protection of vital interests of the data subjects,

-public interest,

-overriding interest of the controller

These six legal grounds apply alternatively and not cumulatively. This does not exclude the possibility of two or more legal grounds to apply at the same time

2.5 What is considered valid consent under the GDPR

When it comes to personal data processing in particular, individual consent is arguably the most important legal ground for processing personal data lawfully.

The General Data Protection Regulation regulates consent in several articles. In particular:

A definition of consent is provided under article 4(11) of the GDPR: consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Recital 32 of the GDPR further clarifies the specific criteria which individual consent should meet: "Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided".

Conditions for consent are listed in **article 7 of the Regulation**. In more detail:

- the controller shall be responsible to demonstrate that the data subject has consented to processing of his or her personal data;
- if consent is given in the context of a written declaration, which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters;
- the data subject shall be free to withdraw his/her consent at any time;
- When the performance of a contract is conditional on consent to the processing of personal data that is not necessary for the performance of that contract, it should always be examined whether the consent has indeed been provided freely;

Children's consent, in particular, is regulated under **article 8 of the Regulation**. The article specifically deals with children's consent in relation to information society services. **Recital 38** clarifies the above by stating that "Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child".

Furthermore, as **regards special categories of personal data**, article 9 of the GDPR specifically mentions that the data subject needs to provide his/her explicit consent to the processing of this category of personal data in order for the general prohibition of non-processing to not apply.

2.6 Processing of personal data in research

Prior to the GDPR, Directive 95/46 recognised research as an important area of public interest justifying derogations from the general rules[1]. It left data protection in the areas of health and medical research largely to Member States to legislate nationally. The GDPR however deviated from this approach and introduced a more specific model for regulating personal data processing that takes place for research purposes.

Recital 159 of the GDPR states that, where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. Therefore, each of the principles under article 5 of the GDPR apply to all data processing including processing for research purposes. The GDPR assumes a broad conception of research, including technological development, fundamental and applied research and privately funded research and 'studies conducted in the public interest in the area of public health.

The special regime in the GDPR for scientific research is handled specifically under Article 89. The article sets the safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and reads as follows:

1. 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 this Regulation, 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.

[1] See for instance Recital 34 to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (replaced by the GDPR): "…Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in areas such as public health and social protection - especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system - scientific research and government statistics; whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals"

Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs".

Article 9(2)j of the Regulation introduces another exception when processing of special categories of data is conducted in the context of scientific research. The article in particular permits derogations to the prohibition of the processing of special categories of data when the purpose of scientific research is met. The article reads as follows: "Paragraph 1 shall not apply if one of the following applies: processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".

It is therefore evident that the GDPR assigns to scientific research a special regime, but otherwise leaves it to Member States to regulate it through national (GDPR implementing acts). Accordingly there have been few guidelines or comprehensive studies on the application of data protection rules to research. On this basis, the EDPS published a preliminary opinion in an effort to highlight the challenges in the application of the GDPR to scientific research[2] .

The opinion points out that "All the provisions above outline a special regime for scientific research and demonstrate that research occupies a privileged position within the GDPR. This flexibility afforded to Member States through the provisions cited above, absent harmonised EU law except in a few areas (such as for clinical trials, see Section 5.2 above), means that the full extent of this special regime is not precisely delineated. Nevertheless, the special regime cannot be applied in such a way that the essence of the right to data protection is emptied out, and this includes data subject rights, appropriate organisational and technical measures against accidental or unlawful destruction, loss or alteration, and the supervision of an independent authority. Personal data which are 'publicly available' - such as those collected from social media sites - are still personal data. Any limitations to fundamental rights in law are to be interpreted restrictively and cannot be abused. It might be considered abusive for instance for a research organisation to interpret these special provisions in the GDPR as allowing the retention of personal data for indefinite periods and to deny data subjects rights to information. Further work is taking place on these questions within the EDPB and at national level".

[2] See https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf

2.7 Rights afforded to individuals (data subjects) under the GDPR

The rights of the data subjects are regulated in articles 13-21 of the Regulation and can be summarised as follows:

- The right to information
- The right to access the data
- The right to rectification
- The right to erasure (the right to be forgotten)
- The right to restriction of processing
- The right to data portability
- The right to object

a. The right to information

The right to information is regulated in two articles, namely Articles 13 and 14. Distinction is made between cases where the information was obtained from the data subject and other cases. In this context, article 13 regulates the case where personal data have been collected form the data subject. In this case, the controller shall at the time when personal data are obtained, provide the data subject with the following information:

a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

b) the contact details of the data protection officer, where applicable;

c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

e) the recipients or categories of recipients of the personal data, if any;

f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

Paragraph 2 of Article 13 lists the additional information the controller needs to provide to the data subject when collecting his/her personal data, such as the period for which the personal data will be stored, the existence of the right to request access to the data or erasure, the right to withdraw consent at any time etc.

Article 14 lists the information to be provided to the data subject where personal data have not been obtained from the data subject itself. Paragraph 5 of article 14 sets some exemptions of the controllers' obligation to provide information, for instance when the provision of such information proves impossible or would involve a disproportionate effort or where personal data must remain confidential etc.

b. The right to access the data

The right of access by the data subject is regulated under article 15 of the Regulation. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him/her are being processed and if yes, access to such data as well as information regarding, among others, the purpose of processing, the recipients to whom the data have been or will be disclosed the existence of the right to request rectification, the right to lodge a complaint and others, the right to request rectification etc. Paragraph 3 of article 15 sets the subject's right to request a copy of his/her personal data from the controller.

It is noted that the right to rectification is regulated separately in article 16. In particular, the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.

c. The right to erasure (right to be forgotten)

Article 17 of the Regulation grants individuals the right to have their personal information deleted by data controllers, if specific conditions, as these are listed in its paragraph 1, are met. For instance, the personal data have been unlawfully processed or they are no longer necessary in relation to the purpose for which they were collected, or the data subject has withdrawn his/her consent and others. In the event that the controller has made such data public, reasonable steps (including technical measures) will be taken to notify controllers who are processing the personal data accordingly. Finally, the "right to be forgotten" (actually, to erasure of data) will not be applicable if it contrasts with the rights of freedom of expression and information as well as for several other, more expected, legal grounds (compliance with a legal obligation, public interest, archiving purposes, etc., as set in paragraph 3).

d. The right to restriction of the processing

Article 18 of the Regulation regulates the right to restriction of the personal data processing. The conditions under which a data subject may exercise his/her rights are listed in the first paragraph of article 18 and include, for instance, the contest by the data subject of the accuracy of the personal data processed by the controller or the claim that the processing is unlawful and therefore the data subject opposes the erasure of his/her personal data. Recital 67 mentions some methods the controller may use to restrict the processing of personal data, such as, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website.

e. The right to data portability

Data portability is dealt with under article 20 of the GDPR and includes the data subject's right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. The right to data portability is provided to data subjects under two conditions:

a. the processing is carried out by automated means;

b. the processing is based on consent or on a contract.

f. The right to object

The right to object is laid down in Article 21 of the GDPR. Recital 69 of the Regulation clarifies the conditions under which a data subject may object to his/her data being processed. The recital reads as follows: "Where personal data might lawfully be processed because 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, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject". In other words, the exercise by an individual of its right to object to its personal data being processed by a controller essentially includes a balancing of rights and legitimate interests: on the one hand an individual is interested in having its data no longer processed and on the other hand a controller may have an interest in continuing to process such data despite the individuals' objections.

2.8 Security of personal data

Security of personal data is regulated under Section 2 of the GDPR and in particular under articles 32-34.

Article 32 deals with security of processing and sets the **controller's and the processor's obligation to implement technical and organisational measures to ensure a level of security including among others**:

a. the pseudonymisation and encryption of personal data;

b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c. the ability to restore the availability and access to personal data in timely manner in the event of a physical or technical incident;

d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.

Another parameter of security of personal data is the notification of a personal data breach to the supervisory authority. Data Breach Notifications are regulated by article 33. A "personal data breach" is defined in the text of the GDPR, in Article 4(12), as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed". When this happens, controllers shall, according to article 33, par. 1 "without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay". The obligation of notification burdens the processor as well, who, shall notify the controller without undue delay after becoming aware of a personal data breach (article 33 par.2). Paragraph 3 lists the minimum information the notification must contain, such as the nature of the data breach, the name and contact details of the data protection officer, the likely consequences of the personal data breach and the measures taken or proposed to be taken by the controller to address the personal data breach.

Finally, the communication of a data breach to the data subject is regulated under article 34. This obligation burdens the controller in any case where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in article 33(2). Paragraph 3 of article 34 sets the conditions under which the communication to the data subject is not required. In particular par. 3 reads as follows "The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner"

3 Ethics in research

3.1 How to conduct research ethically: Setting the regulatory landscape

a. Regulation EU 1291/2013

All EU funded projects must comply with specific ethical principles. The main instrument that sets these principles is the Regulation establishing Horizon 2020[3] . In its article 19 in particular, under the title "Ethical Principles", the Regulation describes the main ethics' concerns and principles that should be taken into consideration when conducting research. In more detail, according to the Regulation, the ethical framework in Horizon 2020 is defined by five ethical principles:

- All the research and innovation activities carried out under Horizon 2020 projects shall comply with ethical principles and relevant national, Union and international legislation, including the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights and its Supplementary Protocols. Particular attention shall be paid to the principle of proportionality, the right to privacy, the right to the protection of personal data, the right to the physical and mental integrity of a person, the right to non-discrimination and the need to ensure high levels of human health protection;
- Research and innovation activities carried out under Horizon 2020 shall have an exclusive focus on civil applications;
- In Horizon 2020 projects the following fields of research shall not be financed: research activity aiming at human cloning for reproductive purposes; research activity intended to modify the genetic heritage of human beings which could make such changes heritable; research activities intended to create human embryos solely for the purpose of research or for the purpose of stem cell procurement, including by means of somatic cell nuclear transfer;
- Research on human stem cells, both adult and embryonic, may be financed, depending both on the contents of the scientific proposal and the legal framework of the Member States involved. No funding shall be granted for research activities that are prohibited in all the Member States. No activity shall be funded in a Member State where such activity is forbidden;
- The fields of research set out in paragraph 3 of this Article may be reviewed within the context of the interim evaluation set out in Article 32(3) in the light of scientific advances[4].

b. The European Code of Conduct for research integrity

The European Code of Conduct for Research Integrity[5] is a useful tool in evaluating and establishing the values that any type of entity operating in an organised social environment should apply. The Code applies to research in all scientific and scholarly fields and has been recognised by the Commission as the reference

[3] Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC

[4] Article 32(3) of the Regulation states that "By 31 December 2017, and taking into account the ex-post evaluation of the Seventh Framework Programme to be completed by 31 December 2015 and the review of the EIT, the Commission shall carry out, with the assistance of independent experts, selected on the basis of a transparent process, an interim evaluation of Horizon 2020, its specific programme, including the European Research Council (ERC), and the activities of the EIT [….]".

[5] http://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf

document for research integrity for all EU-funded research projects, as well as a model for organisations and researchers across Europe.

The Code clarifies that good research practices are based on fundamental principles of research integrity, which include:

- Reliability in ensuring the quality of research, reflected in the design, the methodology, the analysis and the use of resources;
- Honesty in developing, undertaking, reviewing, reporting and communicating research in a transparent, fair, full and unbiased way;
- Respect for colleagues, research participants, society, ecosystems, cultural heritage and the environment;
- Accountability for the research from idea to publication, for its management and organisation, for training, supervision and mentoring, and for its wider impacts.

The aforementioned principles govern the internal process of conducting research and could be used as a guidance for researchers in their research work and in their collaboration with each other. They, therefore, warrant the integrity of the research and they should apply together with the ethical principles, as these shall be elaborated below under section 3.2.

c. The European Commission's "ethics issues table"

Identifying ethical issues in research is the first and most important step in order to safeguard that the research in question will indeed be conducted in accordance with any applicable ethical principles. In this context, the European Commission has issued guidelines on how to complete an ethics self-assessment[6] . The document covers most of the issues that may arise in research projects and provides useful guidance on how to perform an ethics self- assessment.

The Commission's guidelines address the following fields or categories of research:

- Research on human embryos and foetuses;
- Research on human beings;
- Research on human cells or tissues;
- Research which involves processing of personal data;
- Research involving animals;
- Research involving non-EU countries;
- Research that may adversely affect the environment, or the health and safety of the researchers involved;
- Research involving goods, software and technologies covered by the EU export Control regulation No 482/2009 (dual use items);
- Research that has an exclusive focus on civil applications;

[6] https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf

- Research involving or generating materials, methods, technologies or knowledge that could be misused for unethical purposes.

For each category mentioned above the Commission's document provides an ethics issues checklist, as well as a list of information and documents that need to be provided together with the checklist. The ethics' issues table is considered up to date, however, any participant in research should be ready to identify and address any other ethical issues that are not covered by the Commission's guidance.

3.2 List of ethical issues that may be encountered during research

Based on the information included on the aforementioned EU official documents on the ethical aspects of research, we could conclude that the following ethical issues should be specifically addressed for the purposes of this report:

- Informed consent;
- Privacy/confidentiality;
- Vulnerable subjects including patients, elderly and children;
- Civil application and dual use;
- Personal data;
- Potential misuse of research findings;
- Information security.

Each of these issues is followed by an indicative list of measures that could be undertaken in order to minimise the infringement of ethical principles when conducting research in the context of H2020 EU projects

3.2.1 Informed consent

a) Under what conditions is consent considered valid?

Informed consent of the subjects participating in a research project is the first parameter that should be taken into consideration from all involved parties.

Consent for research purposes should meet specific conditions in order to be valid. In particular:

- It should be freely given;
- It should be obtained in advance;
- It should be in writing;
- It should be informed, based on adequate and accurate information;
- It should always be freely withdrawn.

The European textbook on ethics in research[7] , published by the Commission, provides a tripartite definition of 'valid consent' according to which valid consent must include the following three elements:

- **Adequate information**
- **Voluntariness**
- **Competence**

Adequate information refers to both the quantity and the quality of information provided to the data subjects. Participants should be clearly informed of the research goals and possible adverse events. Voluntariness means in practice that the consent must not result from coercion, manipulation, or undue inducements. Finally, competence suggests that the person giving the consent has sufficient mental competence or capacity to understand and retain relevant information about the research, communicate his or her views on the research accordingly.

b) Informed consent under the Charter of Fundamental Rights and the Convention for the Protection of Human rights.

There is substantial official guidance that refers explicitly to respect for free and informed consent. For instance, the Charter of Fundamental Rights of the EU[8] , in its, article 3 (Right to the integrity of the person) states that "1. everyone has the right to respect for his or her physical and mental integrity. 2. In the fields of medicine and biology, the following must be respected in particular: the free and informed consent of the person concerned, according to the procedures laid down by law". Article 5 of the Council of Europe's Convention for the Protection of Human Rights and Dignity with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine[9] states that: "An intervention in the health field may only be carried out after the person concerned has given free and informed consent to it. This person shall beforehand be given appropriate information as to the purpose and nature of the intervention as well as on its consequences and risks. The person concerned may freely withdraw consent at any time".

The above are not meant to lead to the misconception that consent is required only in medical research. Informed consent is an ethical issue that should be addressed in all research fields where humans are involved. Individual consent as a condition for lawful processing of personal data as well as the ethical issues associated with such processing is elaborated below under 2.3.4.

c) Information to be provided to research subjects according to the Ethics for Researchers report by the Commission

The European Commission has published an ethics for researchers report[10] where it lists the information that should be provided to the research subjects before they participate in the research. This information includes:

[7] https://ec.europa.eu/research/science-society/document_library/pdf_06/textbook-on-ethics-report_en.pdf
[8] See https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN

[9] See https://rm.coe.int/168007cf98

[10] See http://ec.europa.eu/research/participants/data/ref/fp7/89888/ethics-for-researchers_en.pdf

- The purposes of the research and information about what will happen with the results of the research;
- The experimental procedures and a detailed description of the involvement of the participants, including the expected duration, and all the relevant procedures;
- All foreseeable risks or discomforts expected to occur for the research subjects during and after their participation;
- All benefits to the participants or to others which may reasonably be expected to occur;
- The insurance guarantees for the participants during and after participation and information on the foreseen treatments and compensations. Alternative procedures or treatments that might be advantageous to the participant need to be disclosed;
- Procedures in case of incidental findings;
- A description of the procedures adopted to guarantee the participant's privacy: the levels of confidentiality, the measures to protect the data, the duration of the storage of the data and what will happen with the data or samples at the end of the research;
- Contact details for researchers who can be contacted at any time to answer pertinent questions about the research and the participant's rights and that can be contacted in the event of a research related injury;
- A clear statement that the participation is voluntary, that the refusal to participate will involve no penalty or loss of benefits to which the participant would otherwise be entitled and that the participant may decide, at any time, to discontinue participation without penalty;
- Information about the organisation and funding of the research project.

d) Informed consent form and content under the Commission's Guidance for Horizon 2020 Programmes

The European Commission in its document entitled "Horizon 2020 Programme Guidance How to complete your ethics self-assessment[11]" provides some useful guidelines on informed consent in case of research that involves human participants. In more detail, as far as informed consent is concerned, the document states that participation must be entirely voluntary and that participants informed consent must be obtained and clearly documented in advance. In this context:

1. Participants must be given an informed consent form and detailed information sheets that:

- Are written in a language and in terms they can fully understand;

- Describe the aims, methods and implications of the research, the nature of the participation and any benefits, risks or discomfort that might ensue;

- Explicitly state that participation is voluntary and that anyone has the right to refuse to participate and to withdraw their participation, samples or data at any time without any consequences;

- State how biological samples and data will be collected, protected during the project and either destroyed or reused subsequently;

[11] See https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf

- State what procedures will be implemented in the event of unexpected or incidental findings (in particular, whether the participants have the right to know, or not to know, about any such findings).

2. Researchers must ensure that potential participants have fully understood the information and do not feel pressured or coerced into giving consent.

3. Participants must normally give their consent in writing (e.g. by signing the informed consent form and information sheets). If consent cannot be given in writing, for example because of illiteracy, non-written consent must be formally documented and independently witnessed.

4. Especially for the case of children or other persons unable to give consent, e.g. certain elderly populations, persons judged as lacking mental capacity the document suggests that researchers must obtain informed consent from the legally authorised representative and ensure that they have sufficient information to enable them to provide this on behalf and in the best interests of the participants. Whenever possible, the assent of the participants should be obtained in addition to the consent of the parents or legal representatives. Participants must be asked for consent if they reach the age of majority in the course of the personal data processing and/or research, as appropriate.

e. Consent in the context of personal data processing and consent of human participants; what are the differences?

In the recent opinion published by the EDPS[12], an effort is made to draw the line between consent as a legal basis for data protection – as this was analysed above- and consent of human participants. It is worth quoting the relevant paragraph: "There is clear overlap between informed consent of human participants in research projects involving humans and consent under data protection law. But to view them as a single and indivisible requirement would be simplistic and misleading. Consent serves not only as a possible legal basis for the activity, it is also a safeguard - a means for giving individuals more control and choice and thereby for upholding society's trust in science. There may be circumstances in which consent is not the most suitable legal basis for data processing, and other lawful grounds under both Articles 6 and 9 GDPR should be considered. However, even where consent is not appropriate as a legal basis under GDPR, informed consent as a human research participant could still serve as an 'appropriate safeguard' of the rights of the data subject. Under what conditions such informed consent might be deemed an appropriate safeguard is still unclear. Certainly, innovative forms of consent in research activities, like tiered and dynamic consent, are promising practices that should be further encouraged and developed. The notion of consent in the two areas requires further discussion between the research community and data protection experts as part of a wider reflection on the role of consent and respect for individuals in the area of scientific research in the digital age".

Informed consent is also regulated under Regulation No 536/2014[13] on clinical trials. Its article 29 states that "1. Informed consent shall be written, dated and signed by the person performing the interview referred to in point (c) of paragraph 2, and by the subject or, where the subject is not able to give informed consent, his or her legally designated representative after having been duly informed in accordance with paragraph 2. Where the subject is unable to write, consent may be given and recorded through appropriate alternative means in the presence of at least one impartial witness. In that case, the witness shall sign and date the informed consent document. The subject or, where the subject is not able to give informed consent, his or her legally designated representative shall be provided with a copy of the document (or the record) by which informed consent has been given. The informed consent shall be documented. Adequate time shall be given

[12] See footnote 2 above

[13] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC Text with EEA relevance

for the subject or his or her legally designated representative to consider his or her decision to participate in the clinical trial.

2. Information given to the subject or, where the subject is not able to give informed consent, his or her legally designated representative for the purposes of obtaining his or her informed consent shall:

a. enable the subject or his or her legally designated representative to understand:

i) the nature, objectives, benefits, implications, risks and inconveniences of the clinical trial

ii) the subject's rights and guarantees regarding his or her protection, in particular his or her right to refuse to participate and the right to withdraw from the clinical trial at any time without any resulting detriment and without having to provide any justification;

iii) the conditions under which the clinical trial is to be conducted, including the expected duration of the subject's participation in the clinical trial; and

iv) the possible treatment alternatives, including the follow-up measures if the participation of the subject in the clinical trial is discontinued;

b. be kept comprehensive, concise, clear, relevant and understandable to a layperson

c. be provided in a prior interview with a member of the investigating team who is appropriately qualified according to the law of the Member State concerned

d. include information about the applicable damage compensation system referred to in Article 76(1) and

e. include the EU trial number and information about the availability of the clinical trial results in accordance with paragraph 6.he information referred to in paragraph 2 shall be prepared in writing and be available to the subject or, where the subject is not able to give informed consent, his or her legally designated representative.

4. In the interview referred to in point (c) of paragraph 2, special attention shall be paid to the information needs of specific patient populations and of individual subjects, as well as to the methods used to give the information.

5. In the interview referred to in point (c) of paragraph 2, it shall be verified that the subject has understood the information

6. The subject shall be informed that the summary of the results of the clinical trial and a summary presented in terms understandable to a layperson will be made available in the EU database, referred to in Article 81 (the 'EU database'), pursuant to Article 37(4), irrespective of the outcome of the clinical trial, and, to the extent possible, when the summaries become available.

7. This Regulation is without prejudice to national law requiring that both the signature of the incapacitated person and the signature of his or her legally designated representative may be required on the informed consent form.

8. This Regulation is without prejudice to national law requiring that, in addition to the informed consent given by the legally designated representative, a minor who is capable of forming an opinion and assessing the information given to him or her, shall also assent in order to participate in a clinical trial.

Informed consent of research participants is the main tool human beings participating in research have in their hands for the protection of their freedoms and rights. It is no wonder therefore why the conditions of informed consent are set thoroughly in different regulatory instruments.

Acquiring a valid informed consent of the research participant and keep this consent valid throughout the process should be the main concern of all parties involved in research.

3.2.2 Privacy/confidentiality

a) Definitions

Privacy and confidentiality are considered related issues in research ethics and two of the main principles that need to be observed when conducting research. Defining both terms is the first step in order to understand what the ethical implications of non-respecting or violating these principles would be.

Privacy is a qualified fundamental human right and as such it appears in many official documents. For instance:

- The 1948 Universal Declaration of Human Rights[14], specifically protects territorial and communications privacy. Article 12 states: No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks.

- The European Convention on Human Rights[15] in its Article 8 states that: 1. Everybody has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

- The Charter of Fundamental Rights of the EU[16] in its article 7 entitled respect for private and family life mentions that "Everyone has the right to respect for his or her private and family life, home and communications".

According to the Commission's "European Textbook on Ethics"[17] , privacy is the protection of:

- control over information about oneself;
- control over access to oneself, both physical and mental;
- control over one's ability to make important decisions about family in order to be self-expressive and to develop varied relationships.

As pointed out in the same text "These three elements are widely considered to be the most important aspects of privacy because of the way that breaches in these areas may affect us. Threats of information leaks, threats to our control over our bodies, and threats to our ability to make our own choices about our lifestyles and activities all make us vulnerable and fearful of being taken advantage of by others".

Confidentiality on the other hand focuses on the protection of information. The obligation of confidentiality may derive from a legal obligation, for instance the existence of a contract for the protection of the information disclosed between the parties (non-confidentiality agreement) or on the basis of a

[14] https://www.un.org/en/universal-declaration-human-rights/
[15] https://www.echr.coe.int/Documents/Convention_ENG.pdf
[16] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT
[17] See footnote 7 above

specific relationship between the parties involved, with the most common being the lawyer-client relationship or the doctor-patient relationship. In research particular, confidentiality is associated with trust. Participants should be confident that their personal information should be safe and confidential throughout the process and of course for as long as it is deemed appropriate after the research ends, depending on the nature of such confidential information and the rights of the persons that might be violated in the event of a disclosure. Similarly, project partners should be confident that information exchanged during the Project will not be leaked to third parties or unlawfully used.

b) How can the principles of confidentiality and privacy be respected in research?

It is evident that issues of privacy and confidentiality can arise in all forms of research involving human subjects and the gathering of information about them.

Privacy has to be respected when researchers acquire information about their subjects including their decision to take part in the research in the first place. Some of the measures that need to be undertaken by researchers when conducting their research are:

- acquire the research subject's informed consent. As already mentioned, informed consent is perhaps the most important step in warranting that the research will be conducted in an ethical manner. The subject needs to be informed about the research, its purpose, its potential outcome and any other parameters related to it;
- the subject needs to be always aware that he/she is part of a research;
- warrant that participation in research is the result of free will (special caution when vulnerable groups are involved);
- the subject should be free at all stages of the research to withdraw from the process;
- apply data protection mechanisms especially when sensitive data or vulnerable groups of people are involved;
- safeguard research subjects' dignity and autonomy throughout the process as a direct aspect of their privacy.

As far as **confidentiality** is concerned, this principle refers to how researchers and project partners may communicate the information they acquired from the research subjects. The main challenge is to find the right balance between dissemination of research results and respect for the participants right to the protection of information.

In any event breach of confidentiality could be hindered by acquiring the subject's consent to disclose his/her confidential information or by anonymising the personal information and disclose it in an anonymised form or through entering of confidentiality clauses or agreements.

3.2.3 Vulnerable subjects

a) Definition of vulnerability

Participation of humans in research raise, as we have already demonstrated ethical concerns, let alone when human subjects belong to "vulnerable groups". What do we mean though by vulnerability, what extra

challenges these groups of people create and what are the measures that need to be undertaken in order to safeguard their rights and freedoms?

The definition of vulnerability is necessary before going any further answering the issues mentioned in the previous paragraph. It seems that, so far, there is no single and commonly accepted definition of vulnerability. In this context, vulnerability is classified as one characteristic of people unable to protect their own rights and welfare. Another definition defines vulnerable groups as groups that include captive populations (prisoners, institutionalised, students etc), mentally ill persons, aged people, children, critically ill or dying, poor, with learning disabilities, sedated or unconscious. Sometimes vulnerable participants are understood as those who are unable to give valid consent either due to lack of competence or because of circumstances which cast doubt upon its voluntariness. The World Health Organisation defines vulnerability as the degree to which a population, individual or organisation is unable to anticipate, cope with, resist and recover from the impacts of disaster of the most explicit accounts is that of the Council for International Organisations of Medical Sciences[18] , which defines vulnerable persons as "those who are relatively (or absolutely) incapable of protecting their own interests". **The key elements however in all these definitions is that the vulnerable person is at higher risk of harm or exploitation than others would be in a similar situation and/or is less able than others to protect themselves from harm or exploitation**.

The Commission in its European Textbook on Ethics in Research[19] refers to this matter as follows: Part of understanding and applying the concept of vulnerability will therefore be to consider what additional factors might make a research subject vulnerable. Three main areas stand out as indications of subjects' vulnerability:

- Subjects who lack competence will be unable to protect their interests by choosing to give or withhold consent;
- If the voluntariness of the subjects' consent is compromised, this may similarly prevent them from choosing to give or withhold consent in a way that would protect their interests;
- The physical (or psychological) condition of some subjects leaves them especially liable to harm, for example as a result of frailty through age, disability, or illness.

b) Specific measures to protect vulnerable groups of people when participating in research

The general rule that should apply in all research projects involving vulnerable groups is that such involvement must be absolutely necessary for the specific purposes the research serves and even in this case ought to be restricted to the best extent possible. In other words, vulnerable groups should participate only when the specific research cannot be carried out with persons who are less vulnerable. Special justification for their involvement should always be provided. In the event that vulnerable groups participate in research, there are some further safeguards that need be implemented in order to minimise the exposure of these groups to factors that threaten their rights. Some examples include:

- the research should be designed in such a way to respond to their needs or priorities;
- the research has benefits for the subject that override the disadvantages;

[18] https://cioms.ch/
[19] https://ec.europa.eu/research/science-society/document_library/pdf_06/textbook-on-ethics-report_en.pdf

- improve the quality of consent by understanding what their incompetence consists of and how additional information could help them understand the scope and the purpose of the research;
- if acquiring consent is not an option, find alternatives to consent such as:

  a) gaining the subject assent; assent is not a substitute for consent, however it could be used as a means to respect the individual's autonomy to the extent he/she possesses it;

  b) use family or legally appointed representatives to make decisions on their behalf;

  c) rely on an advance statement that is a statement that has been prepared before the subject became incompetent;

  d) adopt measures to minimise the subjects' inconvenience;

  e) facilitate and simplify the opt-out process (vulnerable subjects should be able to leave the research at any time and without extra formalities).

- Undertake extra measures for the protection of these people personal information (given their vulnerability, their information will most probably be of a sensitive nature)
- Hire professionals to assist vulnerable subjects throughout the process if necessary (psychologists, doctors etc.)

3.2.4 Civil application and dual use

a) Definitions

European research funding is only possible for research with an exclusive focus on civil applications, excluding thus any military use. Article 19(2) of Regulation 1291/2013 establishing Horizon 2020 states that: "Research and innovation activities carried out under Horizon 2020 shall have an exclusive focus on civil applications.

With regard to the concept of dual use, this is used to describe technologies and products that are generic and can address the needs of both civil and military end-users. These are commonly referred to as "dual-use" goods or technologies.

b) How do these notions apply to research

Dual use technologies are not by default excluded from EU funding on the condition however that they are exclusively focused on civil applications. The relevant paragraph from the Commission's explanatory note[20] on exclusive focus in civil applications reads as follows: "Research activities aimed at the development or improvement of dual use technologies or goods can be financed through H2020, provided that the research is fully motivated by, and limited to civil applications".

The Commission, in its Guidance note[21] , clarifies that if the research is intended to be used in military application or aims to serve military purposes, it cannot be funded under Horizon 2020. At the same time, it clarifies the features of the actors involved in the research activity is not a factor that should determine whether a research activity qualifies for funding. In particular, the fact that military partners or partners active in the defence industry or in military research participate in a project does not preclude the funding

[20] https://ec.europa.eu/research/participants/portal/doc/call/h2020/ds-04-2015/1645170-explanatory_note_on_exclusive_focus_on_civil_applications_en.pdf
[21] https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/guide_research-civil-apps_en.pdf

of the research. Additionally, the research topic should not affect the judgement of whether a research qualifies for funding either. In this context, the Commission's explanatory note mentions that projects involving the defence industry or military organisations are not automatically excluded from funding. Research on defence related subjects may still qualify for funding, as long as its aims are exclusively focused on civil applications. The decisive factor according to the Commission as this is included in the explanatory report reads as follows: "In order to determine whether a project or proposal meets the conditions laid down in the regulation, the objective(s) of the proposed activity have to be assessed. If the technologies/products/services concerned are intended to be used in non-military activities or aim to serve non-military purposes, they will be considered as having an exclusive focus on civil applications. Research directed towards military applications is excluded from funding".

Focus on civil application is an issue that should always be checked by all participants in research projects when conducting their ethics assessment.

3.2.5 Protection of personal data

a. Definition of personal data

According to the GDPR)[22] and in particular its article 4 (1) "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". The relevant legal analysis has taken place above, under Chapter 2.

b) How is the right to data protection addressed in ethics in research

Data protection is both a fundamental human right and a crucial issue when ethics in research are examined. The right to data protection is enshrined in the EU Charter of Fundamental Rights and the Treaty on the Functioning of the European Union. As a result, individuals' right to the protection of their personal data is undisputable. Research subjects in particular, should always be assured that this right is respected. This can be achieved if researchers provide research participants with information regarding any parameter of processing of their personal data, for instance what kind of data are being collected, for what purpose, how long will they be stored for, will they be destroyed if no longer needed, who is the processor and his contact details, how the data subject can have access to such data, is the data subject informed about their right to be forgotten etc. Particular attention should be paid to research involving special categories of data or data concerning children or vulnerable groups of people are being processed, as well as when complex processing of personal data takes place as such processing operations may pose higher risks to the rights and freedoms of data subjects.

It is no surprise therefore that protection of personal data of research subjects requires this much of attention. It is in this context that the Commission has issued a report of Ethics and Data Protection[23] in an effort to help researchers identify and address ethics issues as early as at the stage of preparing their research proposal.

[22] See Regulation (EU) 2016/679 of the European Parliament and the of the Council https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en

[23] https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf

c) How to identify and address data protection issues in research

As with all ethical issues in research, data protection issues may also be addressed through the conduct of a data protection risk assessment. In any event all EU-funded research projects should comply with data protection legislation and more particularly with the GDPR. In this context the commission has recorded a list of indicators of data processing operations that may entail higher ethics risks. These are:

• processing of 'special categories' of personal data (formerly known as 'sensitive data') such as racial or ethnic data, political opinions, religious or philosophical beliefs, genetic, biometric or health data, sex life or sexual orientation, trade union membership

• processing of personal data concerning children, vulnerable people or people who have not given their consent to participate in the research;

• complex processing operations and/or the processing of personal data on a large scale and/or systematic monitoring of a publicly accessible area on a large scale or involvement of multiple datasets;

• data processing techniques that are invasive and deemed to pose a risk to the rights and freedoms of research participants, using camera systems to monitor behaviour, data mining, profiling individuals or groups, using artificial intelligence to analyse personal data or techniques that are vulnerable to misuse; and

• collecting data outside the EU or transferring personal data collected in the EU to entities in non-EU countries.

Whenever personal data are collected directly from research participants, the best way to proceed is to seek their informed consent by means of a procedure that meets the minimum standards of the GDPR. This requires consent to be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the subject's agreement to the processing of their personal data. Furthermore, if the data processing entails potential risks to the data subjects' rights and freedoms, they must be made aware of these risks during the informed consent procedure.

Other ways to mitigate the ethical concerns arising from the use of personal data is to anonymise them or pseudonymise them.

3.2.6 Potential misuse of research findings

a) Definition – Research vulnerable to misuse

A definition of misuse of research findings is included in the Commission's guidance note[24] , as well as in the explanatory note[25] issued also by the Commission. On this basis, "potential misuse of research refers to research involving or generating materials, methods, technologies or knowledge that could be misused for unethical purposes".

According to the note the research most vulnerable to misuse is research that:

- provides knowledge, materials and technologies that could be channelled into crime or terrorism;

[24] https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/guide_research-misuse_en.pdf
[25] https://ec.europa.eu/research/participants/portal/doc/call/h2020/fct-16-2015/1645168-explanatory_note_on_potential_misuse_of_research_en.pdf

- could result in chemical, biological, radiological or nuclear weapons and the means for their delivery;
- involves developing surveillance technologies that could curtail human rights and civil liberties;
- involves minority or vulnerable groups or develops social, behavioural or genetic profiling technologies that could be misused to stigmatise, discriminate against, harass or intimidate people.

Research misuse should not be confused with "research misconduct". Given that research misconduct could raise ethical concerns, if occurred, it is useful to include its definition in the context of this report. Research misconduct is defined as: fabrication, falsification and plagiarism. Falsification is defined as the misrepresentation of results. Fabrication is defined as the reporting on experiments never performed. Plagiarism is defined as taking the writings or ideas of another and representing them as one's own.

b. Identifying and addressing potential misuse

The Commission's guidance note has addressed the issue by listing a number of questions that need to be answered in order for potential misuse to be identified. In particular:

- Could the materials/methods/technologies and knowledge concerned harm people, animals or the environment if modified or enhanced?

- What would happen if they ended up in the wrong hands and knowledge involved or generated would end up in the hands of malevolent individuals?

- Could they serve any purposes other than the intended ones? If so, would that be unethical?

If there is a positive answer to one of the above questions, the next step is to try and address the risk by implementing specific measures.

Again, the explanatory note mentions several ways to mitigate risks, such as:

- Take additional security measures, e.g. physical security measures, classification of certain deliverables, compulsory security clearance for those involved in the project;

- Take additional safety measures, e.g. compulsory safety training for staff;

- Adjust the research design, e.g. use dummy data;

- Limit dissemination, e.g. by publishing only part of the research results, regulating export, etc.

3.2.7 Information security

a) Definition

Information security encompasses all measures taken to protect the information processed within a system (e.g. electronic, physical) from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Information security is represented by the so-called security triad (CIA triad) i.e., confidentiality, integrity, and availability of information. ENISA in its guidelines for SMEs on the security of personal data[26] processing has defined these three security principles as follows:

[26] https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

- **Confidentiality** is defined as the "property that information is not made available or disclosed to unauthorised individuals, entities, or processes". In practice, all the measures implemented to ensure confidentiality are designed to prevent the information from being accessed by unauthorized individuals, entities or processes, while ensuring that the authorised individuals, entities or processes have access to it.

- **Integrity** is defined as the property of "accuracy and completeness". In that sense, integrity implies maintaining the consistency, accuracy, and trustworthiness of information, over its entire life cycle. Data must not be changed in transit and measures must be undertaken to ensure that data cannot be altered by unauthorised individuals, entities or processes.

- **Availability** is defined as the property of "information being accessible and usable when an authorized party demands it". This means that the systems used to store and process information, as well as the information communication channels are all functioning correctly.

b) Ethical concerns regarding information security in research

Information security raises major ethical concerns especially in research activities. The reason for this is that valuable information could possibly be at stake that include both personal data- in many cases sensitive- and research findings. Safeguarding therefore the integrity, confidentiality and availability of such information should always be a high priority for everyone involved in research. Insufficient information security could lead to breach of confidentiality and information integrity. The consequences of confidentiality violations as well research findings misuse could lead to serious complications and have been analysed above in the relevant sections.

Information security could be achieved through the adoption of adequate organisational and technical measures, as well as through the use of security policies. For instance use of GDPR compliance tools to collect, process and store research subjects; personal data, encrypt the research data and/or the devices on which they are stores, avoidance of free services that may use the participants information for their own purposes, ensure that all parties involved in research (partners, collaborators) implement appropriate information security policies. A best practice in order to address issues of information security is to conduct a sound information security risk management, if proportionate with the processing particularities.

4 The NAIADES project: ethical and legal compliance

4.1 Project's description

a. General

Managing water resources is becoming increasingly important and Smart Water Management (SWM) has become a critical need. NAIADES's vision is to support the modernization and digitization of water sector by providing a holistic solution for the control and management of water ecosystems. The NAIADES Ecosystem envisions transforming the water sector through automated and smarter water resource management and environmental monitoring, achieving a high level of water services in both residential or commercial consumers, exploiting the efficient use of physical and digital components of water ecosystem.

NAIADES will apply on large datasets from water utilities in three European countries, including (i) the water consumption in both retail and corporation efficiency, (ii) the confidence of water consumers (potentially including special groups as ageing, disabled persons and children), by measuring the water quality in residential buildings, offices and public infrastructures (mall), (iii) the safety and reliability through the detection of warning signs from equipment failures and maintenance report, and (iv) personalized persuasive feedback and recommendation services provided to the NAIADES App Users aiming to enhance public awareness on water consumption and usage savings, and promote user engagement in water conservation activities.

b. The NAIADES architecture: The NAIADES app in particular

The NAIADES architecture consists of the technical architecture and the detailed technical specifications of the smart water management ecosystem, as well as of the accompanying services. The technical architecture will specify the components (including software modules) comprising the NAIADES system, along with the structuring principles driving their integration. In particular, the NAIADES architecture will include novel prototypes and business model variant, IoT and artificial intelligence technologies (optimisation, prediction, diagnosis). Therefore, during the NAIADES project a wide number of different technologies, modules and subsystems will be developed and designed.

One of the NAIADES ecosystem parameters is the NAIADES app, which is a personalised water behavioural change application, accessible via smartphones and tablets, which will enhance public awareness on water consumption and nudge behavioural water efficiency. The NAIADES app will facilitate water end-users to know how much water is consumed, to get personalized recommendations of action plans for water conservation, along with an estimation of their impact on water use and user comfort and finally to be nudged towards water conservation-related behavioural change. Data captured from smart meters/sensors and user's feedback will feed persuasive visualizations, while personalised insights will be provided through water usage comparisons with other similar users of the application that are efficient in terms of water consumption.

It is clarified that this analysis focuses on two aspects of the NAIADES ecosystem, namely the NAIADES pilots and the NAIADES app. The NAIADES architecture, as mentioned above, includes several modules, which however, given the early stage of the project, was not considered in a finalized enough format for a legal analysis to be applied to it. The NAIADES architecture will thus be evaluated in the context of deliverable D1.6 that is due on month 36 and which will include final remarks regarding any legal and ethical issues pertaining to the project.

The choice of examining the pilots and the app in particular is based on the fact that it is important to ensure at this early stage that the pilots will run safely, in full compliance with the legal and ethical principles in effect. With regard to the app, given that this will be the tool used by the end-users, it was essential to safeguard from the very beginning that the necessary legal provisions and ethical requirements would be taken into account while developing it.

The above choice was vindicated after the initial submission of this deliverable report D1.4, because it was requested after the interim review and respective report, that it be clarified "*how the decision of going for the development of a Global Water Observatory, instead of predictive AI analytics for consumer confidence, downsized the need for the Ethics structure and to which extent the data gathered by the Consortium are still ethically relevant*". This was a re-alignment in the project's work that came after submission of the original report (v.1.0) and was consequently not taken into consideration. However, at the request of the project said change was realized under WP5, specifically T5.4. In the relevant deliverable D5.7 it is clarified that the data to be collected within the context of the Global Water Observatory are as follows:

- Ews: Derived from filters defined by use-cases;
- Twitter / social media: Derived from collected (public) tweets;
- Weather: Collected from regions defined by use-cases;
- Research: Relevant to interests of use-case partners;
- Indicators: Collected from Spain and regions, not related to individuals.

The above justify any downsize in the project's ethics structure, because, visibly, the sources of the data as regards the Observatory are public and non-personal whereas the NAIADES project was originally prepared to deal with predictive AI analytics. However, it needs to be clarified that said change did not affect the compliance mechanism installed within NAIADES, not only out of practical circumstances (an already ongoing mechanism) but also due to the fact that adherence to higher ethical standards will warrant improved compliance, and thus public trust, in the project's findings.

c. The NAIADES pilots

The proposed technology and business framework will be validated through real life demonstrations in three different water management infrastructures. The operational properties of the proposed ecosystem, and overall solution will be validated and evaluated against performance, effectiveness and usability indicators. Water authorities participating in the project's pilot tests will deploy and evaluate the solution at business as usual and emergency situations across various environmental scenarios.

The pilots are:

- CUP Dunarea Braila (CUP), a public utilities company, with over 900 employees, more than 125 years of experience in water supply, sewerage and regional operator with activity on the entire Braila County.

- Ville de Carouge. The city of Carouge is located in the State of Geneva, Switzerland. It counts more than 22.000 citizens. Carouge is the Smart City leader in the Canton of Geneva and has a complete network and IT infrastructure for the Smart City.

- Aguas de alicante (AMAEM) (50/50 (Municipal/Private) manages the urban water cycle of Alicante and the surrounding municipalities. The company supplies water to more than 500.000 inhabitants (700.000 in the summer) through a distribution network of more than 2.000 kilometers.

4.2 The project's particularities

In order to better evaluate the NAIADES project's compliance with ethical principles and with the General Data Protection Regulation, its particularities and special features should be taken into consideration. **The main particularity is that the NAIADES project belongs to the category of Smart and Sustainable Cities (SSC**). In this context, special attention should be given to the personal data processing activities that will take place during the project's duration. On top of that it is anticipated that, as regards the NAIADES app, personal data could potentially be processed and therefore special security measures should be implemented by the project's partners at the stage of designing the application. Informed consent, confidentiality, data protection by design and by default, security of information are some of the issues that will be examined in the context of this report. **It is pointed out that no personal data processing is anticipated to take place during the project's validation through the pilots. It has been made clear by all partners of the NAIADES consortium that any data that will be processed for this purpose will be dummy data or data that do not constitute personal data**. These issues will be examined thoroughly in the sections that follow.

Another issue that needs to be pointed out, which however does not raise any particular concerns, is that three of the partners are located in Switzerland and are considered therefore non-EU countries. Even though Switzerland is not a member of the EU, it implements legislation that meets the requirements of EU legislation and consequently it is considered to be fully compliant for the purposes of the NAIADES project.

4.3 NAIADES and ethics: compliance with ethical principles

4.3.1 The European Commission's checklist

As already mentioned in previous sections of this report, the Commission has issued guidelines on how to complete an ethics self-assessment[27]. To this effect it has developed a checklist that all parties involved in research should address as a first step in the process of identifying any ethical complications in the research they intend to engage in. The checklist includes specific categories of research that are particularly vulnerable to ethics concerns. The table below has been created based on the categories referred to in the Commission's document. If one or more boxes are checked, then special attention should be given as to whether the research in question meet the ethical principles. With regard to NAIADES in particular, the ethics checklist has as follows:

Does NAIADES research falls within any of these categories of research?	YES	NO
• Research on human embryos and foetuses		x

[27] https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf

• Research on human beings		x
• Research on human cells or tissues		x
• Research which involves processing of personal data	x	
• Research involving animals		x
• Research involving non-EU countries		x
• Research that may adversely affect the environment, or the health and safety of the researchers involved		x
• Research involving goods, software and technologies covered by the EU export Control regulation No 482/2009 (dual use items)		x
• Research that has an exclusive focus on civil applications	x	
• Research involving or generating materials, methods, technologies or knowledge that could be misused for unethical purposes		x
• Other ethics issues that should be taken into consideration		x

Based on the above checklist the main ethical concern that needs to be addressed in the NAIADES research focuses on the personal data processing activities that will be conducted through its duration. However, it is considered important to first address all ethical issues referred to in the second part of this report in order to ensure that all ethical issues related to the research in question have been properly evaluated.

4.3.2 List of ethical issues in the NAIADES project

a) Informed consent

The significance of informed consent in all research projects where humans are involved, has been pointed out several times in the first part of this report, both in the context of chapters 2 and 3. Acquiring informed consent from the research participants is absolutely necessary for the research to be conducted ethically and for the rights and freedoms of the research subjects to be respected. It is repeated that valid consent should be:

a. freely given

b. obtained in advance

c. in writing

d. based on adequate and accurate information

e. freely withdrawn

Adequate and accurate information includes the following:

The purposes of the research and information about what will happen with the results of the research.
The experimental procedures and a detailed description of the involvement of the participants, including the expected duration, and all the relevant procedures
All foreseeable risks or discomforts expected to occur for the research subjects during and after their participation
All benefits to the participants or to others which may reasonably be expected to occur
The insurance guarantees for the participants during and after participation and information on the foreseen treatments and compensations. Alternative procedures or treatments that might be advantageous to the participant need to be disclosed
Procedures in case of incidental findings
A description of the procedures adopted to guarantee the participant's privacy: the levels of confidentiality, the measures to protect the data, the duration of the storage of the data and what will happen with the data or samples at the end of the research
Contact details for researchers who can be contacted at any time to answer pertinent questions about the research and the participant's rights and that can be contacted in the event of a research related injury.
A clear statement that the participation is voluntary, that the refusal to participate will involve no penalty or loss of benefits to which the participant would otherwise be entitled and that the participant may decide, at any time, to discontinue participation without penalty.
Information about the organisation and funding of the research project.

In NAIADES, informed consent forms have already been circulated to the project partners. The project is not anticipated to engage any research subjects during the running of the projects' pilots. However, involvement of the pilots' employees at different stages of the project's execution is possible. Given the

nature of the deployed organisations- they are all large entities that belong entirely or by a percentage to the public domain- it is anticipated that they have in place the necessary procedures and measures for the protection of their employees' rights and freedoms. In case therefore of any employees' engagement, consent form with the information described above, should be acquired in advance if needed. To this effect project partners have been advised (as a best practice) to acquire such informed consent forms from all of their employees involved in the project. It should be noted that in principle no participation of employees of the above organisations, in the form of research subject/participants, is expected to take place during the NAIADES pilots.

In case however of any employees' engagement with the project, a consent form with the information described above, should be acquired in advance.

b. Civil application and dual use

All research activities carried out under Horizon 2020 projects must have an exclusive focus on civil application. The NAIADES project has a clear civil application use. Consequently, any further elaboration on potential dual use is considered unnecessary.

c. Vulnerable subjects

As already mentioned above, no research participants are expected to be engaged for the NAIADES project. Ethical concerns regarding vulnerable subjects are therefore non applicable. In the event of participation of employees of the pilots, in the capacity however described above, namely not as research subjects but only supportively for the facilitation of the project, it should always be safeguarded that employees belonging to vulnerable groups of people should be treated with respect when participating in the NAIADES project.

d. Privacy / confidentiality

Both principles of privacy and confidentiality should be carefully addressed in all projects when human participation is expected. Again the NAIADES project will not engage any research subjects (as the term has been explained above). In the event that employees of the pilots participating in NAIADES are involved in the process (by for instance providing support or information), it must be made sure that their right to privacy and confidentiality is respected throughout the project. In particular, it must be made clear to them that they take part, even supportively and not as research subjects, in the specific research. Their consent should be acquired in advance and should be kept up to date. Furthermore, basic information about the project should be communicated to them. As long as these persons provide any personal information during their participation in the research, this information should be kept confidential. If there is a need for such information to be disclosed, the person should be informed in advance and his/her consent for such disclosure should be acquired in writing. In the same context, it should be made sure that all parties involved in the project, who may receive such confidential information are bound by confidentiality obligations. Finally, it is very important that the necessary precautions have been taken in order to keep such information confidential even after the project has expired. The principle of confidentiality and how it could be protected in the context of the NAIADES project is closely connected to the data protection principle and therefore it will be examined thoroughly below in the relevant section.

e. Protection of personal data

Protection of personal data is a major ethics issue that needs to be addressed in all EU-funded projects. In the case of the NAIADES project in particular, the possibility of personal data being processed should be assessed. When discussing the project's particularities under 4.2 above, the following points are made:

a. As far as the NAIADES research is concerned, as well as the pilots participating in the project, it has been demonstrated that no personal data will be processed. With regard to the employees of the partners and of course of the pilots that may provide assistance during the project's execution, specific measures should be adopted in order for the processing of these persons personal data to be lawful and for the rights of the data subjects regarding their personal data to be respected.

b. The NAIADES app on the other hand, based on its description and specifications is anticipated to collect and process personal data

The specific measures that should be adopted in order for the NAIADES project to comply with the data protection legislation shall be thoroughly examined below under 4.4. This will help in identifying the risks related to the processing of personal data in NAIADES, as well as in implementing the safest solutions in order to keep these data safe.

f. Potential misuse of research findings

For consistency reasons we list again the types of research that is more vulnerable to misuse according to the Commission's guidance;

- provides knowledge, materials and technologies that could be channelled into crime or terrorism;
- could result in chemical, biological, radiological or nuclear weapons and the means for their delivery;
- involves developing surveillance technologies that could curtail human rights and civil liberties;
- involves minority or vulnerable groups or develops social, behavioural or genetic profiling technologies that could be misused to stigmatise, discriminate against, harass or intimidate people.

Given the NAIADES project's description, it is very unlikely that its research findings will be misused even in the case of them ending up in the wrong hands.

g. Information security

Information security has three dimensions: confidentiality, integrity, and availability of information. Information security plays an important role when it comes to research ethics. Keeping information, provided or generated during a project, safe, in other words safeguarding the integrity, confidentiality and availability of such information, should always be a high priority for everyone involved in research. During the NAIADES project it is anticipated that important information will be collected, such as water consumption data, quality of the water, chemical components of the water and other. It is therefore very important that this information will be secured and protected against loss or destruction. Information security could be achieved through the adoption of adequate organisational and technical measures. A further analysis is provided below under 4.4.

4.4 NAIADES and the protection of personal data; Compliance with the GDPR

4.4.1 NAIADES pilots

As elaborated above, when it comes to personal data processing in the NAIADES project, a distinction should be made between the NAIADES research/NAIADES pilots and the NAIADES app.

Close collaboration with the NAIADES partners and exchange of information has indicated that no personal data will be processed during the running of the pilots. Any data collected and processed will focus on the quality and the quantity of the water consumed by the pilots. In the same context any conclusions regarding the water consumption of the deployed pilots will not be personalised, as no data of identified or identifiable water consumers will be used. At the same time any feedback regarding water consumption, as well as any suggestions to enhance public awareness on this issue and any recommendations in order to implement efficient water management, will be provided at a collective level, addressing each pilot in an impersonalised form and it will not target individuals. It is therefore concluded that no personal data will be processed during the NAIADES project, as far as water consumers/end users are concerned.

With regard to the employees' personal data that may be processed for the project's purposes, in the context explained in the previous sections, such processing should be performed in compliance with the GDPR. In particular personal data must be processed lawfully, fairly and in a transparent manner, they must be collected for a specified explicit and legitimate purpose, they must be adequate, relevant and limited to the purpose of processing, they must be accurate and up to date, they must be stored for no longer that is necessary for the purposes of processing and they must be processed in a manner that ensures security of personal data.

For the project's purposes and to the extent that any personal data are being processed, it is essential that NAIADES applies the processing principles indicated by the GDPR in order to safeguard that the data subjects are always informed about the processing of their personal data and their rights related to such processing and that they have provided their explicit consent for such processing. In addition, it should be transparent to any persons participating in the project that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed (the principle of transparency).

Finally, and as regards the persons rights in the context of the NAIADES project, all rights the GDPR provides for data subjects should be respected throughout the project's duration. In more detail, the right to information and access to personal data the right to erasure and right to object should be safeguarded. NAIADES must make sure that, in the event of any personal data being processed for its purposes, the abovementioned rights of the data subjects will be respected and that data subjects will be enabled in exercising them. NAIADES must inform in advance the data subjects of the basic information referred to in article 13 of the GDPR, such as its contact details (as controller) and, where applicable, of its representative, the purposes of the processing for which the personal data are intended, as well as the legal basis for the processing, the recipients or categories of recipients of the personal data, if any etc. Other information, according to paragraph 2 of Article 13 would be the period for which the personal data will be stored, the existence of the right to request access to the data or erasure, the right to withdraw consent at any time, etc. Furthermore, NAIADES should always be ready to enable data subjects to exercise the right to be forgotten and the right to object.

It is pointed out that given that the data subjects participating in NAIADES do so in their capacity as employees of the pilots partners, it is expected by the respective pilot partners to have taken the necessary measures, as data controllers, to safeguard the protection of the personal data of their employees within their organisations and to respect their rights as data subjects.

4.4.2 The NAIADES app

The NAIADES app will, based on its specifications, interfere with processing of personal data. In particular, the application that will be introduced in the context of the project is described as a personalised water behavioural change application which will:

- be accessible via smartphones and tablets;

- enhance public awareness on water consumption and nudge behavioural water efficiency;

- facilitate water end-users to know how much water is consumed;

- give water end-users personalized recommendations of action plans for water conservation, along with an estimation of their impact on water use;

- nudge water end-users towards water conservation-related behavioural change;

- through data collection from smart meters/sensors and together with user's feedback provide persuasive visualizations;

- Provide personalised insights through water usage.

With these parameters in mind, the NAIADES app falls within the scope of the GDPR and should consequently comply with its provisions. All its functions lead to the conclusion that processing of end-users' personal data will be conducted. In order to enable and enhance GDPR compliance during the project execution, guidance will be provided to the application developers to abide by GDPR requirements (particularly privacy by design and by default- see below under 4.4.4). Obviously however the final GDPR compliance exercise will have to take place after the project ends, at the time of actual deployment of the application.

4.4.3 Security of processing in the context of the NAIDES project

Whenever and however personal data are being collected in the context of a project, it is the researchers ethical and legal obligation to ensure that participants' information is properly protected. This is fundamental to safeguarding their rights and freedoms, and minimising the ethics risks related to the data processing.

Security of the processing is regulated under section 2 of the GDPR and in particular under articles 32-34. Article 32 lists the measures the controller and the processor shall implement in order to ensure a level of security appropriate to the risk. These measures include among others:

a) the pseudonymisation and encryption of personal data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In addition to the organisational and technical measures, another parameter for ensuring security is the process of notifying a personal data breach to the supervisory authority, as this is described in article 33 of the GDPR. Finally, security is completed with the process of article 34 of the Regulation, namely the communication of a personal data breach to the data subject.

The GDPR requires all data controllers and processors to implement appropriate technical and organisational measures to ensure a level of data security that is commensurate to the risks faced by the data subjects in the event of unauthorised access to, or disclosure, accidental deletion or destruction of, their data (art.32 GDPR).

NAIADES should provide details of the technical and organisational measures that will be implemented to protect the personal data processed in the course of the NAIADES research. Such measures may include the pseudonymisation and encryption of personal data, and policies and procedures to ensure the confidentiality, integrity, availability and resilience of processing systems and other.

The Commission has published a list with 10 do's and don'ts that research participants should have in mind when it comes to data security[28].

	DO's	DON' ts
1	use GDPR-compliant tools to collect, process and store research subjects' personal data;	collect data on a personal device such as a smartphone without ensuring that they are properly protected (e.g. consider the implications of automatic back-ups to the cloud, and the device's security features);
2	take communications security seriously, and devise and implement dedicated protocols for your project as necessary;	use free services that may use your participants' data for their own purposes in lieu of payment, or collect data or communicate with research participants via social media platforms without first assessing the data protection implications;
3	check the terms and conditions of all of the service providers you use (software, applications, storage, etc.) to process personal data within your project, in order to identify and mitigate risks to the data subjects	use unencrypted email, SMS or insecure 'voice over IP' platforms to communicate with vulnerable participants or those who may be subject to state surveillance;
4	encrypt your research data and/or the devices on which they are stored, and ensure that keys/passwords are appropriately protected; and	expose personal data to unauthorised access or use when accessing them remotely (e.g. by using insecure wifi connections) or travelling to countries where your devices may be inspected or seized; and
5	consult your DPO or a suitably qualified expert for advice on how to achieve a level of	assume that your research partners, collaborators or service providers have appropriate information security and data

[28] See https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf

	data security that is commensurate to the risks to your data subjects.	protection policies without checking that this is the case.

The above list will be communicated to the project partners, adapted as appropriate to the project's requirements.

4.4.4 The NAIADES app and data protection by design and by default

a. What is data protection by design and by default?

The GDPR, for the first time, addresses data protection by design as a legal obligation for data controllers and processors. Furthermore, it introduces the obligation of data protection by default and establishes the protection of personal data as a default property of systems and services.

The term "Privacy by Design" means "data protection through technology design." Behind this is the thought that data protection in data processing procedures is best adhered to when it is already integrated in the technology when created.

Recital 78 of the GDPR states that the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. These principles are regulated under article 25 of the Regulation which reads as follows:

"Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects".

Data protection by design must therefore be implemented at the time of determination of the means for processing. The "means of processing" ranges from the abstract to the concrete detailed design elements of the processing, such as the architecture, procedures, protocols, layout and appearance. The "time of determination" of such means is when the controller is in the process of determining which means to incorporate into the processing. Once the processing has started the controller has a continued obligation to maintain DPbDD, i.e. continued effective implementation of the rights and principles. The nature, scope and context of processing operations may change over the course of processing, which means that the controller must re-evaluate their processing operations through regular reviews and assessments of the effectiveness of their chosen measures and safeguards.

Data protection by default is regulated under article 25 par.2 which states that:

"The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons".

According to the EDPB guidelines on data protection by design and by default[29], a "default", as commonly defined in computer science, refers to the pre-existing or preselected value of a configurable setting that is assigned to a software application, computer program or device. Such settings are also called "presets" or "factory presets", especially for electronic devices. 40. Hence, "data protection by default" refers to the choices made by a controller regarding any preexisting configuration value or processing option that is assigned in a software application, computer program or device that has the effect of adjusting , in particular but not limited to, the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

b. How to apply the principle in the NAIADES app: Specific measures that should be considered to this effect.

As already demonstrated above, it is anticipated that the NAIADES app will collect and process personal data. It is undisputable therefore that the principle of data protection by design must apply. The NAIADES app should, at the early stage of its "architectural building", be designed in such a way that any personal data processing will be conducted with respect to data subjects rights and freedoms. In other words, privacy measures and privacy enhancing technologies (PETs) should be directly embedded into the design of the NAIADES app.

Measures to achieve data protection by design could include:

• the pseudonymisation or anonymisation of personal data;

• data minimisation

• applied cryptography (e.g. encryption and hashing)

• using data-protection focused service providers and storage platforms; and

• arrangements that enable data subjects to exercise their fundamental rights (e.g. as regards direct access to their personal data and consent to its use or transfer).

As regards pseudonymisation of personal data in particular, ENISA published, in January 2019, a Recommendation on shaping technology according to GDPR provisions, an overview on data pseudonymisation[30]. The report discusses the benefits of pseudonymisation for data protection and addresses some techniques that may be utilised for pseudonymisation.

ENISA has also published a report on Privacy and Data protection by Design- from policy to engineering[31]. The aim of the report is to explore and indicate how privacy by design can be implemented with the help of engineering methods. Even though the report was published in 2014, hence 6 years have already passed since then, ENISA proposes, among other things, eight privacy design strategies, which are distinguished in two further categories data-oriented strategies and process- oriented strategies. These strategies could provide basic guidelines to the NAIADES partners at the stage of organising their data protection by design policy. According to ENISA, a design strategy describes a fundamental approach to achieve a certain design goal. It favours certain structural organisations or schemes over others. It has certain properties that allow it to be distinguished from other (fundamental) approaches that achieve the same goal.

The eight privacy design strategies included in the report prepared by ENISA are:

[29] See https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf

[30] https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions

[31] https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

- **minimise:** the amount of personal data that is processed should be restricted to the minimal amount possible,

- **hide**: any personal data and their interrelationships should be hidden from plain view,

- **separate**: personal data should be processed in a distributed fashion, in separate compartments whenever possible,

- **aggregate**: personal data should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful,

- **inform**: data subjects should be adequately informed whenever personal data is processed (this connects to the notion of transparency),

- **control**: it governs the means by which users can decide whether to use a certain system and the way they control what kind of information is processed about them,

- **enforce**: it ensures that a privacy policy is in place (this relates to the accountability principle),

- **demonstrate**: a data controller should be able to demonstrate compliance with the privacy policy and any applicable legal requirements.

5 Conclusion

This report begins with the evaluation of the EU regulatory framework on the protection of personal data. The main provisions of the General Data Protection Regulation are presented with special attention been given to the lawfulness of processing and the rights of the data subjects. In addition, the main ethical concerns and risks associated with research are thoroughly examined. In the third chapter of this report the general conclusions and findings derived from the legal/ethical analysis of the two first chapters are applied onto the NAIADES project.

In this context, the project's particularities and requirements in terms of ethical and legal compliance are elaborated and at the same time specific measures are suggested to the project partners with the aim of assisting them in executing the project in a lawful and ethical manner. Personal data protection issues, especially as far as the design of the NAIADES app is concerned, are closely examined. The conclusions of this report, together with the questionnaires that will be circulated to the partners during the project's term, will safeguard that people's rights and freedoms participating or involved in it will be respected at all times. In the same context, specific modules of the NAIADES architecture were not examined under this report on the grounds that they are still under development. A legal analysis regarding any personal data protection issues that may arise out of or in connection to these modules will be included in Deliverable D.1.6 (Ethical Helpdesk Reports-Final), which is due on month 36.

6 References

A Preliminary Opinion on data protection and scientific research, by the EDPO, 6.1.2020 https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf

Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC.

The European Code of Conduct for Research Integrity, published in Berlin by ALLEA, 2017 http://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf

European Textbook on Ethics in Research, European Commisison, DG for Research, 2010 https://ec.europa.eu/research/science-society/document_library/pdf_06/textbook-on-ethics-report_en.pdf

Council of Europe, Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine https://rm.coe.int/168007cf98

Universal Declaration of Human Rights https://www.un.org/en/universal-declaration-human-rights/

Council of Europe, European Convention on Human Rights https://www.echr.coe.int/Documents/Convention_ENG.pdf

Charter of Fundamental Rights of the European Union https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

Horizon 2020 Programme- Guidance, How to complete your ethics self-assessment, February 2019 https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf

ENISA, report on Recommendation on shaping technology according to GDPR provisions – an overview on data pseudonymisation https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions

ENISA, report on Privacy and Data Protection by Design, January, 2015 https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, November 2019
https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf