aqua3S

D2.2 – Preliminary ethics and legal framework

WP2 – User Requirements

aqua3s project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 832876.

Document Information

GRANT AGREEMENT NUMBER	832876	ACRONYM	aqua3S
FULL TITLE	Enhancing standardisation strategies to integrate innovative technologies for Safety and Security in existing water networks.		
START DATE	1st September 2019	DURATION	36 months
PROJECT URL	www.aqua3s.eu		
DELIVERABLE	D2.2 – Preliminary ethics and legal framework		
WORK PACKAGE	WP2 – User Requirements		
DATE OF DELIVERY	CONTRACTUAL June 2020	ACTUAL	June 2020
NATURE	Report	DISSEMINATION LEVEL	Public
LEAD BENEFICIARY	TRI		
RESPONSIBLE AUTHOR	Peter Wieltschnig (TRI)		
CONTRIBUTIONS FROM	Zachary Goldberg (TRI), Francesca Lombardo (AAWA), Tsanidis Vasileios (RCM), Papadopoulos Nikolaos (RCM)		
ABSTRACT	This deliverable documents the initial ethics and legal risks and framework to be followed throughout the project, including suggested high-level solutions. In doing so, it utilises an impact assessment methodology in order to identify key ethics and legal risks and opportunities before distilling these findings into the preliminary ethics and legal framework, to be used as guidance throughout the aqua3S project.		

Document History

VERSION	ISSUE DATE	STAGE	DESCRIPTION	CONTRIBUTOR
V.1	09.06.2020	Draft	Initial draft	Peter Wieltschnig (TRI)
V.2	10.06.2020	Draft	Review	Zachary Goldberg (TRI)
V.3	11.06.2020	Draft	Amended draft	Peter Wieltchnig (TRI)
V.3	16.06.2020	Draft	First internal review	Francesca Lombardo (AAWA)
V.4	24.06.2020	Draft	Amended draft	Peter Wieltschnig (TRI)
V.5	29.06.2020	Draft	Second internal review	Tsanidis Vasileios & Papadopoulos Nikolaos (RCM)
V.6	29.06.2020	Final	Final version	Peter Wieltschnig (TRI)

Disclaimer

Copyright message

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS/ACRONYMS

API	Application Programming Interface
CCTV	Closed-circuit television
CESCR	Committee on Economic Social & Cultural Rights
CRCL	Crisis Classification
D	Deliverable
DSS	Decision Support System
DPIA	Data Protection Impact Assessment
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EPANET	Environmental Protection Agency Network
E/PIA	Ethics/Privacy Impact Assessment
EU	European Union
EWS	Early Warning System
GDPR	General Data Protection Regulation
ICCPR	International Covenant on Civil & Political Rights
ICESCR	International Covenant on Economic, Social & Cultural Rights
IoT	Internet of Things
JSON	JavaScript Object Notation
SCADA	supervisory control and data acquisition
TRI	Trilateral Research
UAV	Unmanned Aerial Vehicle
UI	User Interface
UN	United Nations
WDN	Water Distribution Network
WP	Work Package

1. Executive summary

This deliverable provides the preliminary ethics and legal framework for the aqua3S project. In doing so, the document looks towards the ethics and legal impacts that might arise during the project and those that might arise in relation to future use and uptake.

The deliverable conducts an initial impact assessment to identify and highlight the key issues that might arise. Following this, it offers high-level solutions that are designed to be followed throughout the project. The deliverable is therefore intended primarily for internal use within the consortium, to assist consortium partners in the development and delivery of a system that meets ethics and legal requirements. However, the deliverable also aims to communicate the ethics and legal issues, risks and opportunities within the aqua3S project to the wider public. Such efforts are designed to facilitate discussion on the ethics of the aqua3S solution and the efforts that the aqua3S project is taking to ensure the responsible and sustainable development of the solution itself.

From the outset, *privacy-by-design* and *ethics-by-design approaches* are to be taken within the aqua3S project. These approaches entail the understanding that privacy and ethical values should be built into the system itself. A core axiom for these concepts is that privacy, ethical, and social issues should be considered early, so that they can be highlighted and made meaningful for designers, developers, and stakeholders. This makes the potential dilemmas and tensions faced by end-users in the uptake of the product visible early-on, so that risks can be mitigated to the greatest extent possible and so that they can be made visible before the exploitation activities for ethically aware future use.

Moreover, the timely and concrete identification of project risks plays a critical role as it will allow for aqua3S partners to mitigate and address them early in the project, during the design stage and well before authorising aqua3S system for operation through the pilots.

Fundamentally, a number of functional and non-functional requirements are already outlined in aqua3S. These recommendations are guided by legal instruments such as the GDPR (General Data Protection Regulation, EU Directive 2016/679/EC) and human rights law, as well as EU societal and ethical values. For instance, issues that are relevant for the project are:

- Privacy-by-design.
- Data minimization and anonymisation/pseudonymization.
- Data storage and sharing.
- Technical and organisational processes in place to allow for the correction and deletion of information.
- Drone national regulatory compliance.
- Security technical and organizational measures.
- Collection of information to allow for the assessment of human vulnerability.
- Notification of the community of the project nature and activities.
- Ensuring that warning messaging is sufficiently tailored to the contexts and needs of the community.
- Non-discrimination

2. Introduction

2.1 Background

This deliverable provides the preliminary ethics and legal framework for the aqua3S project. In doing so, the document looks towards the ethics and legal impacts across the timeline of project development and use of the aqua3S solution. It aims to inform the design considerations before the system is put into use through pilots. The ethics and legal framework will be iteratively developed throughout the lifecycle of the project and culminating in the final ethics and legal framework (D2.5).

2.2 Aim of the Document

This document is primarily intended to assist the consortium partners in the development and delivery of a system that meets privacy, ethical and social requirements. The assessment of ethical and legal issues is on-going through the project, and this initial report is intended to contribute to the groundwork of development, providing a preliminary understanding of the ethics and legal issues that are or may become active in the aqua3S project. This information will then be used as the basis for ethics and legal guidance and monitoring throughout the project as a whole, and specifically within WP2 (User Requirements) and WP9 (Policies, Information Management & Standardisation).

The final version of the ethics and legal framework (D2.5 Due month 32) will be an incremental update, focused on the pilots and exercise phase of the impact assessment and additionally developed alongside WP8 (Pilot implementation, evaluation and training). It will include more detailed recommendations as the technological design and necessary practices become more concrete. Moreover, it will calibrate the recommendations outlined within this deliverable to ensure that they remain relevant and attuned to the project solution as it evolves over time. It will also incorporate additional input from end users to ground the recommendations in end-user practice, in the actual engagement and use of the designed technologies, and in specific, rather than generic, user stories.

2.3 Document outline

The document is divided into sections tailored to specific considerations within the preliminary ethics and legal framework.

Following this introduction, which has set out the general nature and purpose of the deliverable, Section 3 provides a greater insight into the use of an ethics and legal framework. The nature, purpose and methodology of an impact assessment to elicit the particular concerns and potential mitigation measures that are relevant within the framework will be then discussed (Section 4.)

Section 5 provides an introduction to the ethics and legal principles that underline and determine the impact assessment. Section 6 then outlines the nature of the aqua3S solution as well as the technical components that are contained within the aqua3S solution; it then provides an analysis of where the ethics and legal risks and concerns arise within the use of the system, before offering high level recommendations for the mitigation of these risks.

Section 7 distils the issues identified in order to provide the preliminary ethics and legal framework. Within this section, a summary of the key issues identified is provided as well as the framework created by the non-functional requirements.

Section 8 provides the final conclusions, information on the next steps of the ethics and legal activities within aqua3S.

Annex A contains the agenda, as well as the ethics risks and opportunities identified by partners within the consortium's ethics workshop held on 3-4 June 2020. Finally, Annex B contains the aqua3S anonymity protocol as developed within WP11.

3. Establishing and Ethics and Legal Framework

3.1 Purpose and use of an impact assessment

In developing a preliminary ethics and legal framework, attention must be paid to the ways in which the aqua3S project and solution impact ethical and legal considerations. An impact assessment process will be utilised to identify these dynamics, across the project development phase as well as the future application of the solution. The outputs of the impact assessment will then be reviewed and considered in order to guide the development of the ethics and legal framework contained preliminarily within this deliverable and in its final form in D2.5.

3.2 Concept of the Impact Assessment

The Ethical and Privacy Impact Assessment (E/PIA) is a systematic approach to mapping information flows, identifying and assessing risks, and providing a set of possible solutions for technology developers to take into account during the design stage of a system. It provides a framework for addressing ethical and social considerations, privacy challenges, and related data protection legislation. An E/PIA is proactive; it considers future consequences and impacts of proposed actions. It enables ethical- and privacy-oriented solutions to be taken into account during the design phase, and, when necessary, also during the development stage of the system. It ensures that privacy and ethics are key considerations throughout the life cycle of (research) projects and/or programs and that those considerations of privacy and ethics are included in the development process of new technological systems. It is intended to allow intervention and change, rather than just act as a documentary exercise in tracking or assessing privacy harms over time. It is also intended to engage stakeholders and affect the direction of a project from its earliest stages.

The aims of conducting a Privacy Impact Assessment are: better privacy protection, increased transparency of personal information processing technologies and increased accountability and the mitigation of the risks of surveillance systems. It focuses on the potential privacy impacts resulting from a project, policy, programme, service, product or other initiatives and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts (Wright 2012). Within Europe, PIAs (Privacy)/DPIAs (Data Protection) are compulsory under the General Data Protection Regulation (GDPR),[1] necessary for demonstrating compliance with legal and regulatory requirements and overall accountability. Worldwide, they are growing in popularity as effective tools for protecting personal data and privacy (Wright & Friedewald 2013). Several regulatory and data protection authorities have introduced their own recommendations and procedures for conducting PIAs (see for example, Information Commissioner's Office 2014; Commission Nationale de l'Informatique et des Libertés' Open Source PIA Tool[2]).

These assessments have been expanded in a range of related directions, including ethical impact assessments (Wright 2015) and societal impact assessment (Wadhwa, Barnard-Wills & Wright 2015). Considering ethics and societal impact identifies societal concerns, embedded values, and potential

[1] https://gdpr-info.eu/issues/privacy-impact-assessment/
[2] https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

impact of a technology (Verbeek 2011; Nissenbaum 1998; Floridi 1999). The aim is to help designers and end-users become aware of morally opaque features of design and use (Brey 2000). Moreover, ethical values and principles underpin and inform privacy and data protection considerations. If not addressed, these issues can become risks to success and sustainability of project aqua3S outcomes. This also contributes towards informed decision-making, protection of societal concerns, and overall effective risk management strategy (Kloza, Van Dijk, Gellert, Böröcz, Tanas, Mantovani and Quinn 2017).

The objective of the E/PIA process is to increase the reflexivity of the process and of decision-making, not to prescript or pre-define the results of an assessment process. The process encourages researchers to assess their role in the research and innovative process, subjecting their activities and decisions to critical scrutiny. In the process, they learn more about the problem domain and reflect upon the potential impacts of different design moves, diverse user practices, and the possible kinds of knowledge generated considering the ambiguities of real-world experience (Carroll 2000). This opens debates about alternative solutions that facilitate the development of creative risk mitigation strategies and responses that consider the broader picture of technology use in situ.

For technology development projects, the E/PIA acts as a foundational component for achieving meaningful 'privacy-by-design', by providing information to support privacy supporting design decisions.

In this project, the E/PIA process includes:

- Developing an understanding of the aqua3S technology.
- Mapping the information flows; this describes and maps the flows of data within the project.
- Identifying key ethical, legal, social, and privacy risks and related harms.
- Stakeholder consultation, via an E/PIA specific end-user workshop and interviews.
- Analysing requirements for privacy and ethical assumptions that could impede their achievement.
- Observing exercises and demonstrations in order to better integrate the ambiguities and complexities of the domain into the identified risks and recommendations.
- Producing preliminary and final E/PIA reports that consolidate and analyse findings and suggest recommendations.

Conducting an E/PIA can increase the benefits to end-users and society brought by the aqua3S outputs. It can provide a better understanding of the socially desirable impacts and value systems within which aqua3S will be implemented, including how best to maximise these contributions. Potential end-users can be reassured that the project partners had taken into account and addressed privacy, legal, ethical, and social considerations throughout the entire aqua3S development life cycle (i.e. from requirements gathering and design, to the implementation). Such understandings and evidence base contribute towards the success of uptake, support the identification of stronger sustainability opportunities and ensure the increasing of stakeholder and public trust in the technologies and practices produced by aqua3S.

Moreover, while the way ethics and social issues arise depends mostly upon the use of the technology by specific people in specific contexts, in complex socio-technical systems like aqua3S roles and responsibilities of stakeholders overlap and thus new risks arise that are beyond individual or organizational responsibility. This makes it difficult to leave the responsibility to perform impact assessments to the individual or organisation alone, as each individual cannot entirely see their

relation to the whole system in which they act (Perrow 1984; Vaughan 1996). Consequently, ethical impact assessments need to be considered throughout the design of the technology itself.

4. E/PIA scope and methodology

This section of the report sets out the stages and approaches used in the impact assessment.

4.1 Information Flow Mapping

Semi-structured interviews with all 11 consortium technical partners, including simulation partners, were conducted to develop a preliminary map of information flows, showing how the data could be gathered, processed, analysed, stored, and transferred. Additionally, to further this understanding the following information has also been relied upon:

- Information uploaded by each partner on the shared online project space,
- Information provided by consortium partners for the purposes of the deliverables about research ethics (under WP11)
- Weekly end-user and technical partner discussions

The interviews were held with the members of the consortium who are working with data and technology to develop the aqua3S platform, but the structure of the interviews remained open enough to follow relevant points and issues raised by the interviewees. The primary focus was in understanding the high-level information and data flows regarding the path data and information, taken from their original setting to their end users. This process maps the following:

- What information/data is collected.
- How the information/data is collected.
- How it will be used.
- How it is shared and with whom.
- Disclosures.
- Security measures.
- Data quality measures.

The results were used to identify vulnerabilities and risk criteria in relation to the aqua3S system. Each interview lasted for an average of one hour.

The map is contained below at section 5.2.

4.2 Workshop

Trilateral Research Ltd. conducted an ethics workshop with the aqua3S consortium in June 2020. Given travel limitations owing to the Covid19 pandemic, the workshop was held online. It consisted of two identical half-day sessions, with each partner of the consortium attending for one of the two. In attendance were also a member of the external advisory board and an external expert specialising in the law relating to water.

The aim of this workshop was to provide consortium partners with an understanding of ethics and legal principles, in order to better sensitise partners to the ways such principles and values are relevant to the project. To this end, the workshop was used to identify which are potential vulnerable communities to risks such as water insecurity, as well as to assess, analyse, map, and propose high-level solutions thereby minimising and avoid project risks. The workshop was also organised to validate the initial findings on the legal, social and ethical dimensions of the aqua3S system; to identify additional issues through the discussion of end-user use cases and experiences; and to consider

potential solutions from end-user experts through guided discussions between technological partners and end-users.

Five representatives from Trilateral Research were present across the two separate sessions, providing expertise in ethics, privacy and GDPR as well as human rights and international law. In addition to the end user participation in the consultation workshop, all aqua3S technology partners participated in order to shed light on the technical perspectives of the various components being developed within the aqua3S solution.

Participants at the workshop were provided with an introduction to the aqua3S project, an overview of the features, functions and characteristics of the system, as well as of the legal, ethical and social methodology and its initial thematic findings. Collaborative and interactive sessions were held, in order to discuss and validate the initial list of risks identified from research, brainstormed with additional legal, social and ethical considerations, and to discuss the impacts on the different use-case scenarios. Participants then discussed potential solutions to mitigate negative legal, social and ethical impacts, including a brainstorm of potential solutions. The results of these conversations have been included within sections 6 and 7 of this deliverable.

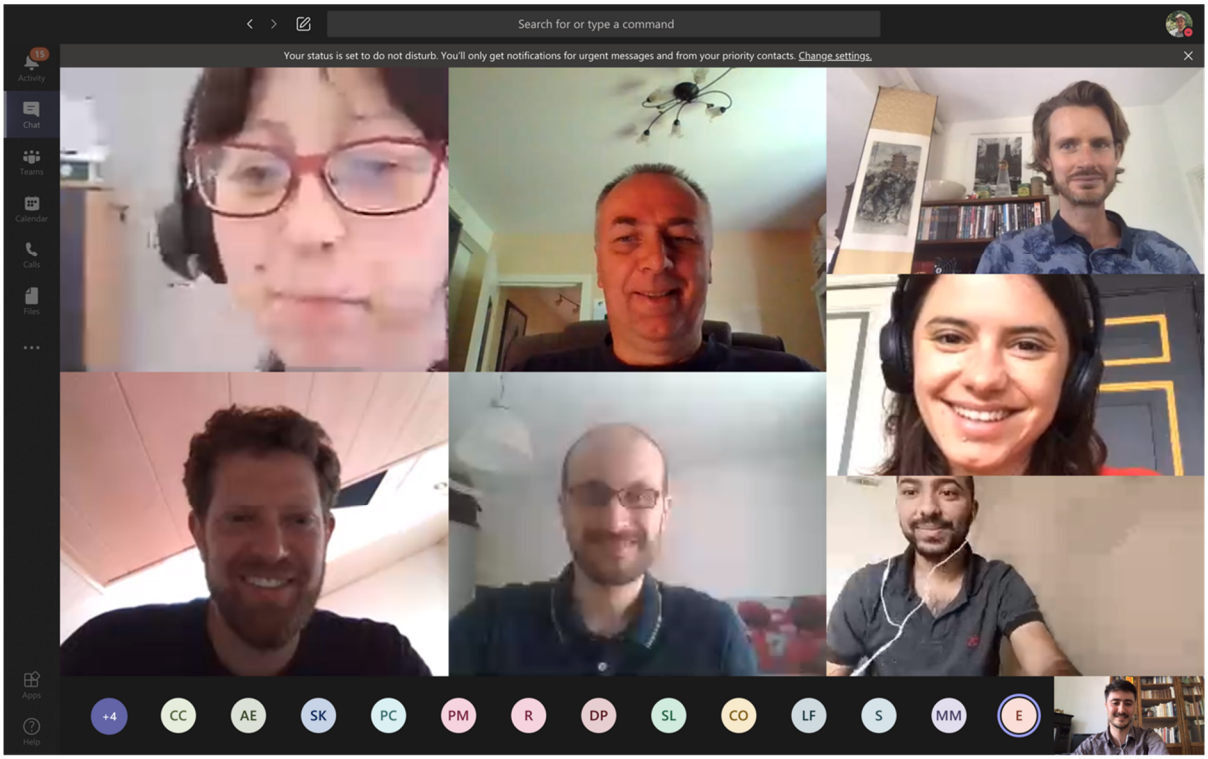

Figure 1. Screenshot of ethics workshop attendees - 3 June 2020

4.3 Review of initial concept, technological components and information flow mapping, user stories, and requirements from a privacy, ethical, legal and social perspective

Impact assessment exercises are often based on a model of the system. However, given that aqua3S is integrating its system through a mix of agile design and pilots, the models used for this preliminary report are high level and fluid. Consequently, the impact assessment process is in a position to influence the resulting model. At this stage, these includes: the initial concepts (derived from the proposal), high level technological components and information flow mapping, pilot storylines from

workshop discussions, and the user requirements. Each of these is reviewed from an impact assessment perspective and potential issues are identified.

4.4 On-going review during development

TRI will participate in the scheduled training exercises where end-users will directly engage with both the project concept and the concrete technologies. During these exercises, end-users will be identified for follow up interviews and to participate in focused virtual discussions between end-users and technology partners. These discussions were used to consider in more concrete detail the identified risks and identify potential solutions. Moreover, TRI will also participate in discussions within the consortium in order to monitor the project's development to identify where other ethics and legal issues may arise. Ultimately, this ongoing review will culminate in the final ethics and legal framework Deliverable 2.5 (M32).

This monitoring process will include the contacting of partners on a monthly basis to request information on ethics and legal issues, including interviewing research participants, the review of project pilots, preparatory measures, and acting as a touchpoint for ethics guidance throughout the course of the project.

5. Introduction to Legal and Ethical Principles

5.1 Introduction

As stated above, this deliverable provides guidance on ethics and legal considerations. However, the meaning of these terms requires further unpacking, as well as other related concepts that are pertinent to the project, in order to understand their content and their scope. Recognising the complexity and breadth of each term, this section provides an overview of a number of concepts, namely: privacy, GDPR and personal data; ethics; and legal compliance relevant to water security. By understanding and appreciating these concepts, it is possible to anchor the aqua3S project in the respect of the underlying values and guide the trajectory of the project and its outputs.

5.1.1 Privacy

Privacy, including information privacy or data protection, is recognised by some scholars and policy makers to be a fundamental human right. These ensuing rights have been enshrined in various international guidelines, accords and frameworks, providing the basis for national laws, policies and international agreements. The United Nations recognised the right to privacy in the Universal Declaration on Human Rights 1948, under Article 12, which stipulates:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

In Europe, rights to privacy, as contained within the European Convention of Human Rights, focus on 'respect for private and family life, home and correspondence' (European Convention of Human Rights, Art. 8.)

Moving on from a descriptive focus on external, especially governmental, interference with individual privacy, participants in contemporary scholarly debates concerning the notion of privacy focus on its normative status. In doing so, they consider it to be either instrumental to the development and exercise of capacities and intrinsic values such as autonomy and dignity. These values principally relate to ethics, and, hence, will be discussed in subsequent deliverables. Additionally, privacy has also been viewed as an intrinsic value itself (e.g. see Becker 2019).

Considered as an instrumental value, privacy is seen to be essential for the development and exercise of other important values. For example, it has been argued that although privacy may have diverse interpretations and numerous contexts in which it is relevant, these interpretations and contexts are unified by possessing pertinence for the exercise of autonomy and for human dignity (Bloustein 1964). Bloustein argues that privacy defines one's essence as a human being, which includes individual dignity and integrity, personal autonomy and independence. Respect for these values is what both grounds and consolidates the concept of privacy. This is the case whether we define it as control over personal space, over information, over one's image, one's movements and associations, or otherwise. Consequently, violations of privacy are ipso facto demeaning to an individual's personality and an offense to human dignity (Kupfer, 1987). Placed in a legal context, the common conceptual thread linking diverse privacy cases about prohibiting dissemination of personal information or non-consensual surveillance is the value of protection against abuses to individual freedom and human dignity.

Considered as an intrinsic value, privacy is seen to be *valuable in itself*, not because it provides for the exercise or development of other values or valuable capacities such as autonomy and dignity. To adopt this perspective, one must narrow the scope of privacy and explain its particular value. This task is a challenge considering the diverse contexts in which privacy appears and assumes normative value. On one account, privacy is argued to be valuable because it establishes intimacy amongst individuals (Fried, 1970; Gerety 1977; Gerstein, 1978; Cohen, 2002). For example, Fried defines privacy as control over information about oneself. He goes on to argue that privacy is necessarily related to an individual's ability to form intimate relationships involving respect, love, friendship and trust. As a consequence, it has intrinsic value in persons' lives.[3] Arguably, love, friendship and trust are only possible if individuals enjoy privacy, recognize its value for each other individual, and choose when to lower barriers of privacy to establish intimacy with others. Practically speaking, if we consider privacy to be intrinsically valuable, then violations of privacy are wrong because simply they violate privacy and not because they are affronts to human dignity or detrimental to the exercise of a person's autonomy.

Privacy can also be interpreted as a public value, meaning that it has value not just to the individual, but also to the democratic political system. For example, Solove argues that privacy promotes and encourages the moral autonomy of citizens, an essential requirement of governance in a democracy (Solove, 2008). Others have argued that privacy is rapidly becoming a collective value in that 'technology and market forces are making it hard for any one person to have privacy without all persons having a similar minimum level of privacy.' (Regan, 1995: 213)

Regarding its public value, there is wide consensus that privacy is an important value for European citizens and residents proving worthy of protection. Significantly, there is also wide consensus among Europeans that they do not possess the amount of control over their privacy as they wish or that they deem necessary. Concerning personal data, and according to Directorate-General for Communication Special Eurobarometer 431 Report on Data Protection only a minority (15%) feel they have complete control over the information they provide online, and 31% think they have no control over it at all. Two-thirds of respondents (67%) are concerned about not having complete control over the information they provide online (Directorate-General Special Eurobarometer 431 'Data protection', 2015). Project partners ought to take seriously what the public perception of the project's tools might be and consider how to reassure users that their privacy is valued, and their personal information will be protected.

To ensure that, the aqua3S project identifies all contexts in which privacy might be relevant for its tools; it is also important to note that privacy can take on different meanings in different contexts, (Nissenbaum, 2009) and that we can distinguish the following seven types of privacy (Finn, et al. 2013).

- Privacy of the person is defined as the right to keep body functions and body characteristics private.

[3] Admittedly, it remains unclear why privacy should be considered under this view as intrinsically valuable rather than instrumentally valuable for intimate relationships, which are intrinsically valuable. However, the goal of this report is not to discuss the philosophical merits of the distinct views, but to present them as possible perspectives in the scholarly landscape.

- Privacy of behaviour and action refers to the ability of the individual to behave and do as they like without being monitored.
- Privacy of communication relates to interception of communications, such as recording and access to e-mail messages.
- Privacy of data and image involves the right of the individual to exercise control over personal data, rather than such data being available to organisations and others by default.
- Privacy of thoughts and feelings refers to the individual's right not to share his or her thoughts and feelings or not to have these revealed.
- Privacy of location and space encompasses the right of the individual to freely move about in public, or semi-public space, without being monitored or tracked.
- Privacy of association refers to the right of the individual to associate with others without being monitored.

Along these lines, privacy can also mean freedom from intrusion, consent, confidentiality, or personal control over what people know about a person.

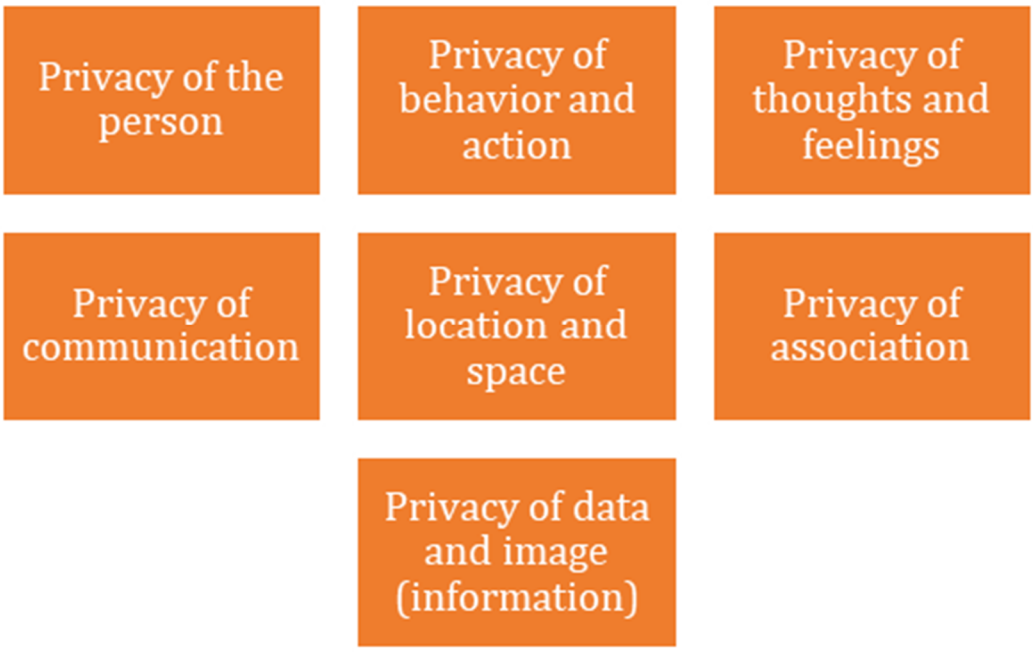

Figure 2. Seven types of privacy

5.1.2 GDPR and Personal Data

The General Data Protection Regulation 2016/679 (GPDR) is the regulatory instrument covering data protection in the European Union and the European Economic Area. The GDPR is applicable when personal data are collected or otherwise processed. Personal data means any information that identifies an individual or renders them identifiable, such as name, location data, identification number etc.

Under the GDPR, data should be collected, used, transferred and stored lawfully (Article 6). This is done when:

- The individual whose personal data is being processed has consented to such processing.
- The processing is necessary for the performance of a contract to which the individual is party.

- The processing is necessary in order to protect the vital interests of the individual whose personal data is being processed or of another natural person. This condition applies to life-or-death scenarios.

Please note that this is a selection of the legal bases that could potentially be used in the aqua3S project. The purposes and the legal base for the processing must be decided in advance (before the start of the processing activities) and cannot be modified in the course of the processing.

- When consent is used as a legal basis for the processing, all criteria that render it valid under the GDPR (Art. 4 (11), Art. 7) should be met. Consent should be able to be withdrawn at any time.
- Relationships between the stakeholders should be thought out, in particular who determines the purposes and the means of the processing.
- Individuals whose data is being processed should be aware of the processing activities, as well as the exact type of data that is being collected from and/ or about them and the purpose for which the processing takes place.
- Data should only be collected for a specific, pre-determined purpose and no further processing, incompatible with the original purpose, is allowed.
- Only the minimum amount of data should be collected.
- Data should not be stored longer than necessary. The retention period should be proportional to the purpose of the processing.
- Security of data stored or otherwise processed should be ensured (through both technical and non-technical measures).
- Data collected and stored should be accurate and up to date.
- Compliance with the GDPR should be able to be demonstrated (through documentation practices).
- Individuals whose data is being processed should be informed about their (data protection) rights and should be facilitated when exercising them. These rights include the:
    - Right to information
    - Right to access data
    - Right to rectify data
    - Right to erasure ('right to be forgotten')
    - Right to restrict processing
    - Right to data portability[4]
    - Right to object to processing

It is not necessary that all rights are awarded to individuals whose personal data will be processed within aqua3S, but that this will depend on the conditions of the processing, the legal basis, the purpose etc. For additional information on how the aqua3S project safeguards these rights, please see

[4] The right for data subjects to obtain that a data controller holds on them in a structured, commonly used and machine-readable format

D1.2 (Self-assessment & data management plan v1) as well as the ethics requirements provided as part of WP11. Other general criteria contained within the GDPR that are relevant to aqua3S include the following:

- Less intrusive **alternatives** should be considered where possible (so that individuals are not identified or identifiable when not necessary).
- Situations where decisions and/ or measures regarding individuals as a result of the information collected about them could be seen as **intrusive** should be analysed in detail
- Situations where technology might affect **third parties**, the way this could happen and how this could be prevented should be analysed in detail
- **Surveillance** in public areas, as an issue that could arise from the project, should be taken into consideration.
- The use of **drones** and the implications they could have on people's privacy and data protection-related rights should be considered.
- **Data sharing agreements** between the stakeholders should be produced, so that information about what data will be shared, how, and to whom it will be shared with is clear and agreed upon.

5.1.3 Ethics

Ethics need to be central in the aqua3S design in order to achieve some of the fundamental objectives of the project, including interoperability and the building of a frame that can bring together diverse actors. Critical and conscientious ethical considerations can thus support a nuanced awareness of data rights and accessibility, which is needed in order to avoid exclusion and repression.

The concept of ethics is not homogenous to all cultures and there are different understandings of ethical philosophies. This is due to moral standards used within society, or within groups in a society, being affected by historical, cultural and geographical differences. However, in brief, ethics is concerned with moral issues, values and principles, as well as practices that are recognized in the daily life of individuals. The European community identity is built on such ethical values as human dignity, fairness, equality and non-discrimination; these values are contained also in its many human rights documents, such as the European Charter of Fundamental Rights. aqua3S partners should be guided by the ethos that technology cannot 'impair fundamental human rights and should contribute to the values they embody', (Wright et al. 2009) as such the use of technology requires us to raise ethical questions.

5.1.4 Security

As security is managed, it has to balance regulations, trade negotiations (who can have the data and at what expense), and intelligence collection (what would be the benefit of knowing and does that outweigh the risks). This often raises questions that need to be actively addressed in design:

What security is guaranteed?

- Privacy?
- Security to share?
- Security to gather, protest, or democratic expression?
- Personal safety?

When can data security be guaranteed?

- When entering?
- While stored?
- While copied and used?

What are the implications when such security cannot be guaranteed?

Whose responsibility it is to keep it secure?

- State?
- Technology?
- Designers?
- Responders?

Moreover, many tools can be used for monitoring urban behaviour of certain users to determine risk to society. Security, here, walks a fine line between surveillance, privacy, consent, pre-emptive risk assessment, and infringing upon human dignity.

5.2 Relevant Principles

The following principles have been identified throughout the literature review on ethical principles, particularly those related to technological innovation and the provision of public services:

- Everyone has a **right to respect for private and family life** (Article 8 of the European Convention on Human Rights) and the State has an obligation to protect it. However, this is a qualified right that can be interfered with in the interest of national security, public safety, or the protection of the rights and freedoms of others.
- Technology should respect a person's **autonomy** and **dignity,** including personal, physical, and mental **integrity**. In this context, the physical and psychological circumstances should be respected.
- When applying/ using/ involving technology, ask yourself:
    - Does the individual have a meaningful choice?
    - Can the individual decline to be monitored?
- All design should strive for **beneficence**, not just better performance.
- The technology used in aqua3S should not infringe any **non-discrimination principles**. According Article 21 of the Charter of Fundamental Rights in the European Union, 'any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited'. This goes hand-in-hand with **equality**, **fairness**, and **impartiality**.
- Situations where decisions and/ or measures regarding individuals as a result of the information collected about them could be seen as discriminatory should be analysed in detail.
- The vulnerable groups that may be affected by the technology should be considered. The concept of **vulnerable groups** include: children, pregnant women, elderly people, malnourished people, ethnic minorities, those living with mental illnesses. Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.

- The technology should not cause **harm**. Harm is understood as both physical and psychological.
- The technology should **benefit** both individuals, both the community.
- The technology should be economically and socially **sustainable**.
- The technology should not isolate users and should be **user-friendly**.
- The technology should not result in decrease in the legitimate exercise of civil liberties and rights, best known as **chilling effect**.
- **Protection of personal data** goes beyond privacy and consent, but also a right to having data fairly processed.
- The technology and required organizational practices should not infringe upon **solidarity** among the users and related stakeholders.
- The technology and required organizational practices should not impede **justice** for the users and related stakeholders.
- aqua3S design should consider how data collected (personal or otherwise) could affect issues of **liability.** Law is vague on what counts as **negligence** or what is acceptable, thus ethical design should consider these issues.
- The technology should build **trust** between users, the users and the public, and between stakeholders and the technology, so that political will not override technological potential.
- The technology and required organisational practices should not enable **mission creep**, where all stakeholders are required to subscribe to one agency's logics in order to use the system.
- Interoperability can lead to many open questions about **responsibility** and **accountability** that, left unaddressed, can put users in tenuous legal situations.
- All acts supported by the tools should be **proportionate** to the situation and need, and no more than necessary.
- The tools should support **stewardship**, intended as the idea of taking care of others' assets and resources.

5.3 Right to Water

The right to water is contained implicitly in various human rights law instruments. The right to water can be seen as implied within rights such as the right to life (International Covenant on Civil and Political Rights (ICCPR) Article 6) and the right to an adequate standard of living and the highest attainable standard of physical and mental health (see Committee on Economic Social and Cultural Rights (CESCR) General Comment No. 15, though this is by no means exhaustive). Explicitly, the right to water has been articulated by the United Nations (UN) General Assembly, acknowledged the human right to water and sanitation in resolution 64/292 adopted in July 2010, calling upon states and international organisations: 'to provide financial resources, capacity-building and technology transfer […] in order to scale up efforts to provide safe, clean, accessible and affordable drinking water and sanitation for all'.[5] Moreover, a number of human rights law instruments have included the right to

[5] Most recently iterated in the Human Rights to Safe Drinking Water and Sanitation Resolution adopted by the UN General Assembly on 19 December 2017, A/RES/72/178. Also General Assembly on 17 December 2015, A/RES/70/169.

water in reference to the needs of specific groups. For instance, the Convention on the Rights of Persons with Disabilities, requires the 'equal access by persons with disabilities to clean water' and the right to water is also contained within the Convention on the Elimination of All Forms of Discrimination Against Women and the Convention on the Rights of the Child. These instruments highlight the vulnerability of certain demographics to water insecurity and the deliberate attention that must be given to ensuring that the right to water is secured.

The CESCR General Comment No. 15 is arguably the fullest delineation of the substantive content of the right to water and is therefore helpful to understand the negative (what government's must refrain from doing) and positive (the deliberate actions that a government must take) obligations that are contained within the right. From this guidance, one can distil the key requirements. Namely the provision of sufficient safe, acceptable, accessible and affordable water. Further, the principle of non-discrimination is articulated within the right to water. Water and water facilities and services must be accessible to everyone, including the most vulnerable or marginalized sections of the population, in law and in fact, without discrimination on any of the prohibited grounds. As such, discrimination is prohibited on the basis of race, colour, sex, age, language, religion, political or other opinion, national or social origin, property, birth, physical or mental disability, health status (including HIV/AIDS), sexual orientation and civil, political, social or other status, which has the intention or effect of nullifying or impairing the equal enjoyment or exercise of the right to water.

Priority in the allocation of water must be given to the right to water for personal and domestic uses. Priority should also be given to the water resources required to prevent starvation and disease, as well as water required to meet the core obligations of each of the rights outlined in the ICESCR. Further, the general comment highlights the need to pay due attention to issues such as environmental hygiene, as an aspect of the right to health under article 12, paragraph 2 (b), of the ICESCR, and agricultural use of water (particularly for disadvantaged and marginalised communities), in a non-discriminatory basis to 'prevent threats to health from unsafe and toxic water conditions.'

Importantly, accessibility does not merely refer to physical accessibility. Rather (and with relevance for the aqua3S project), it demands the accessibility of information, namely the right to seek, receive and impart information concerning water issues. In the EU context, these rights are also being emphasised within the revision of the Drinking Water Directive (98/83/EC) within the EU Parliament following the Right2Water European Citizens' Initiative.

With respect to the right to water, States parties have a special obligation to provide those who do not have sufficient means with the necessary water and water facilities, as well as to prevent any discrimination on internationally prohibited grounds in the provision of water and water services.

Whereas the right to water applies to everyone, States parties should give special attention to those individuals and groups who have traditionally faced difficulties in exercising this right, including:

- women,
- children,
- minority groups,
- indigenous peoples,
- refugees,
- asylum-seekers,
- internally displaced persons,
- migrant workers,
- prisoners and detainees.

In particular, States parties should take steps to ensure that:

The principle of equity underlines the payment of water services, ensuring that these services (whether provided by private or public services) must be affordable for all, including socially disadvantaged groups. Moreover, poorer households should not disproportionately bear the burden of water expenses as compared to more affluent households.

Violations of the obligation to respect follow from the State party's interference with the right to water, including:

- arbitrary or unjustified disconnection or exclusion from water services or facilities
- discriminatory or unaffordable increases in the price of water
- pollution and diminution of water resources affecting human health

Violations of the obligation to protect occur when a State fails to take all necessary measures to safeguard persons within their jurisdiction from infringements of the right to water by third parties.

This includes, inter alia:

- failure to enact or enforce laws to prevent the contamination and inequitable extraction of water
- failure to effectively regulate and control water services providers
- failure to protect water distribution systems (e.g., piped networks and wells) from interference, damage and destruction.

Violations of the obligation to fulfil occur through the failure of States parties to take all necessary steps to ensure the realization of the right to water. Examples include, inter alia:

- failure to adopt or implement a national water policy designed to ensure the right to water for everyone
- insufficient expenditure or misallocation of public resources which results in the non-enjoyment of the right to water by individuals or groups, particularly the vulnerable or marginalized
- failure to monitor the realization of the right to water at the national level, for example by identifying right-to-water indicators and benchmarks
- failure to take measures to reduce the inequitable distribution of water facilities and services;
- failure to adopt mechanisms for emergency relief
- failure to ensure that the minimum essential level of the right is enjoyed by everyone
- failure of a State to take into account its international legal obligations regarding the right to water when entering into agreements with other States or with international organisations.

Whilst the obligations arise at the State must then ensure that these obligations are activated within their jurisdiction – thereby creating obligations at the water service provider level (whether public or private).

Though much literature has been devoted to the right to clean and safe water to the global south, there is relatively little content on the right to water in the European context. This does not suggest that infringements on the right to water do not occur within Europe and that within European member states flagrant violations do not continue. For example, within the literature, issues have been identified in relation to the lack of accessible and safe water in refugee camps, as well as difficulties for Roma communities' access to water across Europe. Further, the adoption of fees for water usage has caused concern over affordability and a disproportionate impact on those who find it

difficult to pay for the stipulated fees. By reviewing these issues, it is possible to identify some core considerations that should be borne in mind when developing the aqua3S system.

5.4 Compliance with Laws, Regulations, Codes and Guidelines

In addition, partners should be mindful of standards contained in, amongst others, but not limited to:

- ISO/IEC 29100:2011
- ISO/IEC 27001:2013
- Universal Declaration on Human Rights 1948
- International Covenant on Economic, Social and Cultural Rights 1966
- The Dublin Statement on Water and Sustainable Development 1992 ('the Dublin Principles')
- European Convention on Human Rights 1953
- General Data Protection Regulation (EU) 2016/679 (GDPR)
- Charter of Fundamental Rights of the European Union 2009
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 2013
- Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1985
- APEC Privacy Framework 2005
- The EU Water Framework Directive 2000/60/EC
- The Drinking Water Directive 98/83/EC
- The Bathing Water Directive 2006/7/EC
- The Environmental Quality Standards Directive 2008/105/EC
- The Urban Waste Water Treatment Directive 91/271/EEC
- The EU Floods Directive 2007/60/EC
- The Nitrates Directive 91/676/EEC

Various international instruments are incorporated into national law by different means. For instance, within the EU context, 'regulations' must be incorporated into domestic law in their entirety. However, directives merely establish goals that States must achieve. The individual State is therefore granted discretion on how they achieve these goals. An example of this is the GDPR, which has been domestically implemented in France through Law n°2018-493 of June 20, 2018. As such, national legislation will be relevant.

Trilateral will base the E/PIA framework on the above standards and legislation and will guide partners though the process of adhering to elements of these standards.

6. Key findings

This section sets out the key risks identified at this stage of the impact assessment, based upon the core concept of aqua3S, pilot use case first storyline, human rights law, data protection law, privacy law, technology and information flow mapping, and user requirements.

Although there is some repetition across these levels, by linking risks to particular elements at multiple levels, this should provide some flexibility for the developers, and allow tracking of issues between concepts, requirements, and (in later versions of the ethics and legal framework) functions.

For example, a privacy or ethical issue might be raised by the way a function has been implemented to meet a user need. In this case, a privacy remedy might include implementing that function in a different way, or meeting the user need through a different function. Alternatively, a privacy or ethical issue might be raised by a need expressed by a potential user.

6.1 Outline of the aqua3S key results

In order to better contextualise the ethical issues, concerns, and possibilities raised in this chapter, the technological components of the system have been organised in the table below to reflect a) their main functions, b) their primary users, and c) the data type they process. These are the technologies that will form the basis for the aqua3S platform. These functions and data types were considered in defining the key categories for the high-level concepts through which to discuss risks. They also help point technology and simulation partners to which issues described in the remaining sections of this chapter could be relevant to their design work.

Key Result (KR01): Optimised sensors for substance detection in water – ICCS/FZU/mirSense
Function(s): The main purpose of the module is to provide the ammonia concentration of a water sample in real time. The user should be able to export the multisense sensor data in a simple file, in a CSV time, that will contain the ammonia concentrations in the water fed to the sensor as a function of time. The user should be able to see (render) a map with following information: aggregated (green, yellow, red) and individual sensor's data in indicated period of time (including forecast future trends). OpenGL and Direct3D formats should be supported. The optimization of the Qascade Cascade Laser (QCL) and the adaptation of its operation in order to detect a given substance, e.g. Ammonium/Ammonia. Current-Voltage characteristic and gain spectrum will be calculated, so that the design corresponds to the required output. Converting concentrations of targets in mg/l to compatible input (ppm) for substances detection with the multisense unit provided by mirSense.
Types of Data Used: Sensor's data that are stored within the computer operating the Graphical User Interface driving the sensor. ASCII files with details of proposed QCL structure, composition of layers, layers length, doping level. Limits of quantification of the chemical and microbiological agents. The data will be available in ASCII format.

Key Result (KR02): Visual content acquisition module – CERTH
Function(s): The main purpose of this component is to identify events threatening water safety or / and security based on collected data. **Satellite** data will be focused on Copernicus products, which will be downloaded and analysed in a periodical interval. The analysis will enhance them with annotation of recognized threats like the existence of oils spills or the concentration of algae bloom. **Drone** images and video streamswill be captured and analyzed on demand. The analysis will enhance them with annotation of recognized threats and detected objects.
Types of Data Used: Satellite data will be downloaded using Copernicus Open Access Hub hub API and stored in the Data Storage module. Drone data must will be submitted to the processing station in a secure manner and stored in the Data Storage module. The dataset will not include sensitive data. The dataset will be stored in the project repository which is hosted in a server of the project coordinator's IT infrastructure. To ensure data recovery in case of accidental deletions, the repository supports version control. Data back-ups will be done according to the internal IT policy of the project coordinator as applicable to all other relevant digital data of the company. Access to the restricted data will only be possible through authenticated access to the repository. More information is available within D1.2 (Self-assessment & data management plan v1).
Key Result (KR03): Social media crawler – CERTH
Function(s): Collects Twitter posts in a real-time manner from citizen observations that are relevant to the subject of water safety and security. After crawling a tweet, further analysis takes place in order to (i) geo-localise them, (ii) filter out irrelevant posts, and (iii) identify fake news. All collected tweets are stored, so end users can search for them anytime.
Types of Data Used: ➢ A list of search keywords ➢ Twitter credentials ➢ Number of collected tweets per day (for event detection)
Key Result (KR04): Data Collection – ICCS
Function(s): A gateway (meshlium) receives sensor data from wireless nodes (Waspmotes) and forwards it via Ethernet or 4G/3G/GPRS protocols depending on the connectivity options available in the area. Data pre-processing and transformation steps can be done also in the gateway.
Types of Data Used: 7 analog inputs, 8 digital input/output, 2 UARTS, 1 I2C, 1 SPI, 1 USB
Key Result (KR05): aqua3S ontology – CERTH
Function(s): The Knowledge Base Service (KBS) consumes the relevant data produced by the analysis modules (satellite / UAVs / Social Media / Sensors) after the harmonization process. The data are transformed in order to be compliant with the aqua3S ontology and stored into the Knowledge Base (KB) in the form of RDF triplets. Within the context of the KB, the available data are correlated and

hidden knowledge is inferred (based on reasoning rules that represent expert knowledge). The correlated data and the inferred knowledge will support the Crisis Classification module and potentially some important detections will be directly forwarded to the end users (to be determined, based on the reasoning rules).

Types of Data Used: Harmonized data from Satellite, UAVs, Social Media, and Sensors

Key Result (KR06): Data management platform and OGC SWE services – ICCS

Function(s): The Data Management Platform, along with the offered OGC SWE services, is the aqua3S module that is responsible for the management and storage of heterogeneous data collected in Task 3.4; These data are required to not only be stored but rather be available to other aqua3S services and modules. The data that are being stored are harmonised in the context of the Task 4.1 and are already translated into OGC compliant resources.

Types of Data Used:

- SensorThings API: Sensor's and drones/satellite data that are stored in the Data Storage module. This data are available via REST API in JSON format.
- OGC WMS: Vector Files and Raster Data (GeoTiff, NetCDF, ArcGrid, ECW, ImageMosaic, JPEG2000, WorldImage) mainly, chaining with other WMS/WFS servers is possible, Gis enabled databases.
- - OGC WFS: Vector Files and Raster Data

Key Result (KR07): Anomaly detection module – UNEXE

Function(s): Data collected at each sensor in the WDN or water source will be analysed using statistical models to detect anomalies based on the historical data at this location.

Data collected at all sensors in the WDN will be analysed using machine learning models or statistical models to localise the anomaly.

As the number of sensors installed in the WDN is usually limited, EPANET model of the WDN can also be used for anomaly detection/localisation by providing detailed hydraulic or water quality simulation time series. EPANET models will also be used to estimate the impact of an incident and support the development of mitigation measures.

If the utility has the network model in another format (e.g. Infoworks) the data need to be transferred to an EPANET model.

Types of Data Used: An EPANET `.inp` file, which describes the network topology, water consumption and control rules, is required for WDN simulations. This is only necessary is the anomaly involves a WDN. In the case of detecting anomalies in sensors alone, this is not needed, but also a combined inference of anomalies (network wise) cannot be implemented. If the existing hydraulic model at the Utility is other than EPANET, then the data will need to be exported to .inp format

Sensor data relating to the anomaly type(s) of interest, including pressure, flow and quality. This will be obtained via API in GeoJSON format.

Key Result (KR08) Developed crisis management scenarios for case studies –

DRAXIS
Function(s): The module that will be developed will consist of a web application that will visualize the results of the crisis management modelling tool, which focuses on (i) modelling of existing infrastructures in the pilot cases, (ii) modelling of water related crisis scenarios for the pilot cases and (iii) modelling of actions that have been taken to manage the crises from past experience. The module will allow the user to develop scenarios for certain crises and provide suggestions for managing the crises, based on the modelling of the pilot cases.
Types of Data Used: TBD
Key Result (KR09): Optimization and parallelization module – USTUTT
Function(s): The objective of this module is to optimize the project's Anomaly Detection Module (developed in KR07 by UNEXE) in terms of serial, as well as parallel performance and efficiency. It will be developed as a plug-in replacement, meaning that it will have the same inputs and outputs as the original Anomaly Detection Module. - The Anomaly Detection Module will collect data at each sensor in the WDN and will analyse using statistical models to detect anomalies based on the historical data at this location. - The Anomaly Detection Module will collect data at all sensors in the WDN and will analyse using machine learning models or statistical models to localise the anomaly. - As the number of sensors installed in the WDN is usually limited, EPANET model of the WDN can also be used for anomaly detection/localisation by providing detailed hydraulic or water quality simulation time series. EPANET models will also be used to estimate the impact of an incident and support the development of mitigation measures. - If the utility has the network model in another format (e.g. Infoworks) the data need to be transferred to an EPANET model.
Types of Data Used: ➢ The output will follow the developments of the Anomaly Detection Module. ➢ The estimated likelihood of incidents occurring in the WDN. ➢ Georeferenced alerts (i.e. quality/pressure status and likelihood of incidents occurring at sensors) that can be displayed in the 3D visualisation module. ➢ EPANET simulation (if it exists) outputs include flow rates in pipes, pressures at junctions, propagation of a contaminant, chlorine concentration, etc., based on the confirmed cause and location of incidents. These simulation data can be exported to the 3D visualisation module to show the extent and severity of the event and intervention management module to develop mitigation measures
Key Result (KR10): 3D Visualisation module for the network – UNEXE
Function(s): The user should be able to see a 3D visualisation of spatial and temporal information (including model outputs and real-time sensor data) that allows them to inspect the system status and see temporal variations. The user should be able to access all of the modules included in the particular case study deployment and see the outputs of these in the 3D visualisation. The 3D visualisation should be integrated with the intervention management model to enable the

user to visualise the consequences of different decision-making or event scenarios.

The 3D visualisation module should allow users to interactively inspect the spatial correlation between hazards, critical infrastructures and their service areas, thus strengthening their understanding and aiding better operation.

Types of Data Used: Spatial information for all infrastructure/assets to be visualised, provided in a standard GIS format (e.g. shapefile or GeoJSON for vector data, GeoTIFF or binary file for raster data). Additional spatial data may include geography, natural environment attributes, topography, demography and climate/weather observations/predictions.

WDN model (EPANET .inp file) if available / if the WDN is to be visualised.

System status data (temporal or static), obtained from sensor measurements or modelling, either directly or from other modules (in JSON format).

Key Result (KR11): Visual analytics module – CERTH

Function(s): The user should be able to see (monitor) a map with current events for emergence of warning signs as well as unexpected events. Satellite images appear as layers on a GIS view, social media images are displayed along with their extracted concepts on the map, and video streams of drones offer additional views of the dams, rivers, lakes and other areas of interest.

The user should be able to customize what he wants to visualize (which data sources, time period) via a user-friendly interface menu.

The user should be able to use module as support for decision making in times of crisis.

Types of Data Used: Drones/Satellite/Video Camera data that are stored in the Data Storage module. Twitter data that are stored in the Twitter Storage module. This data will be available via REST API in GeoJSON or GeoTIFF format.

Key Result (KR12): Intervention Management Model – UNEXE

Function(s): If a WDN model is available, the intervention management model (IMM) can be used to evaluate options for reducing the impact of anomalies within water distribution network (WDN).

Users will be able to forecast future performance of the WDN under different scenarios and operational strategies in real time, by simulating pressure and supply throughout the network, as well as the movement of reactive or non-reactive substances.

Users will be able to define or input operational strategies for evaluation and the intervention management model will facilitate optimisation.

EPANET will be used to analyse hydraulics and water quality in the WDN, accounting for spatiotemporal variation of the water demand, constant or variable speed pumps, and minor head losses for bends and fittings to simulate the flow conditions.

If the utility has the network model in another format (e.g. infoworks) the data need to be transferred to an EPANET model.

The intervention management model will enable users to compare WDS performance under different scenarios and/or operational strategies.

Results from the intervention management model will be output to the 3D visualisation module for

display to the user.

Types of Data Used: An EPANET `.inp` file, which describes the WDN topology, water consumption and control rules.

Sensor data relating to the WDN, including pressure, flow and quality. This will be obtained via API in GeoJSON format.

Scenarios for simulation; these could be in the form of a modified EPANET `.inp` file.

Interventions to be evaluated

Any operational constraints, such as pumps required to be operated simultaneously or exclusively, or valves or pumps out of order; these could be provided as text-based rules (in format used by EPANET) or via options in the user interface.

If the existing hydraulic model at the Utility is other than EPANET, then the data will need to be exported to .inp format.

Key Result (KR13): Crisis classification and Decision Support module – CERTH

Function(s): Crisis Classification (CRCL) module fuses heterogeneous data aiming to provide early warnings or real-time assessments for the crisis severity level, covering the pre-emergency and emergency phase

Types of Data Used: Harmonized data from Sensors.

- Analysis results of the Satellite, UAVs, Social Media analytical modules
- Weather forecasts and 'near' real-time observations for air temperature, precipitation, humidity, wind speed, etc. JSON format
- Prediction for river water level and forest fire danger estimations
- Data from Risk/Impact maps and socio-economic indicators
- Real-time data concerning the indicators for a water supply system
- Historical data for water consumption
- Data related to the current hydraulic situations, ongoing and future maintenance work scheduled in an agenda, operation constraints, unavailable equipment

Key Result (KR14): Guidelines for utility providers to engage communities – CENTRIC

Function(s): The user should have guidelines on how to effectively disseminate information to citizens in times of an emergent or ongoing emergency.

Types of Data Used: Social media data gathered from open and public Facebook and Twitter accounts and pages.

Key Result (KR15): Production of a standardized set of warning messages – CENTRIC

Function(s): The user should have language agnostic (i.e. in manner that is independent of the computer language being used) warning messages to disseminate to citizens for a range of emergent or ongoing emergency.

Types of Data Used: Social media data gathered from open and public Facebook and Twitter accounts and pages. Desk based research.

Key Result (KR16): Emergency Response Plans for the water sector – LHA2
Function(s): First responder emergency response plans for the water sector will be developed for each pilot case allowing responders with different backgrounds and from different jurisdictions to respond effectively together.
Types of Data Used: TBD
Key Result (KR17): aqua3S platform – EVERIS
Function(s): Key Result 17 is aimed at the design of solution architecture and integration of all components of the aqua3S platform. It embraces a set of architecture documents that will be prepared to guide the integration of software components developed in WP3-WP6
Types of Data Used: ➢ KR01-KR13, KR18 provide the technical components that are available for the aqua3S platform. ➢ KR14, KR15, KR16 may provide or have an impact on the functional and non-functional requirements
Key Result (KR18): Interactive user interfaces – DRAXIS
Function(s): Web application that will be used by the end users of aqua3S to interact with the overall system and have access to all the technical solutions of aqua3S. ➢ intuitive and efficient interface based on the needs of the end users ➢ access to all the data that are relevant to each pilot case ➢ access to all the technical components that are applicable to each pilot case
Types of Data Used: The input for the UI will be provided by the following KRs through the aqua3S platform: ➢ KR02 - Visual content acquisition module ➢ KR03 - Social media crawler ➢ KR06 - Data management platform and OGC SWE services ➢ KR08 - Developed crisis management scenarios for case studies ➢ KR10 - 3D Visualisation module for the network ➢ KR11 - Visual analytics module ➢ KR13 - Crisis classification and Decision Support module

Table 1. aqua3S Key Results

6.2 Data Flow Map

The data flow map contains a graphic representation of the key components within the aqua3S system and how they interact holistically, through the various layers of the system.

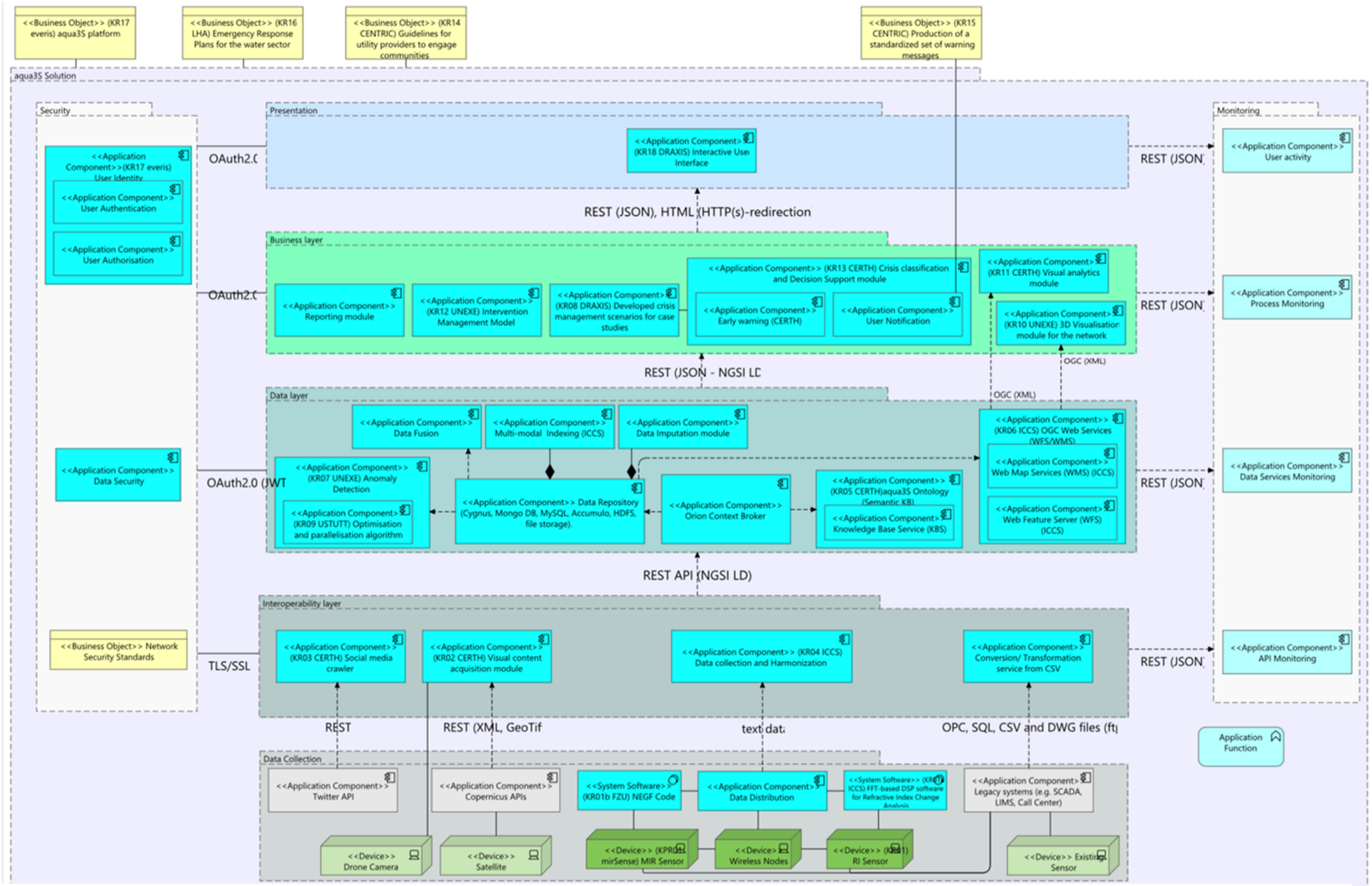

Figure 3. Component architecture map

6.3 Active issues in project development

6.3.1 Personal data and privacy

Whilst some of the data that will be collected is in the public domain, it is also envisioned that at times personal data will be collected. For instance, personal data, including names and contact information, will be needed to record informed consent. The collection and use of personal data for research should be limited to include only that information which is legitimately required in order to complete the specified task. Indeed, from the outset of aqua3S, technical and organizational measures will be implemented to ensure that the principles relating to the processing of personal data as stipulated in GDPR are adhered to. These include the principles of lawfulness, fairness, transparency; purpose limitation; data minimization; storage limitation; accuracy, storage limitation, accountability, integrity and confidentiality (Art. 5.1 of the GDPR). These principles will translate into the following requirements:

- Every data subject has the right to access, question, modify, and rectify all personal data on file. The contact information that data subjects may use to make such requests is contained within the information sheets that is to be provided to all research participants involved in aqua3S (see D11.2)
- Every subject has the right to object to processing of personal data for legitimate reasons as well as a right to object to the use of those data for commercial prospecting, in accordance with applicable regulations. The contact information that data subjects may use to make such requests is contained within the information sheets that is to be provided to all research participants involved in aqua3S (see D11.2)
- Upon lawful request, every subject may receive a copy of the personal data and may amend any personal data which are inaccurate or incomplete
- Secure physical work sites will be used within aqua3S. Access codes will be used for systems storing personal data, as well as the use of password protected files
- Informed consent forms and information sheets on the project and the rights of the data subjects will be provided to research participants in order to ensure that their consent is freely given and that they are aware of their data rights
- Access to files containing personal data is restricted to research teams
- Data used to train the aqua3S system will be anonymised/pseudonymised/artificial
- Sensitive data will also be encrypted
- The minimum of personal information is collected and stored
- Anonymisation and pseudonymization techniques are used in regard to the collection of personal information
- Personal data will only be processed where there is a legitimate basis for doing so. The legitimate bases of each partner who processes personal data will be documented within the project (as has been recorded within D11.8). Where the legitimate basis is no longer applicable the partner will cease processing the personal data.

D1.2 (Self-assessment & data management plan v1) provides more specific information on how data subjects' rights will be met within the aqua3S project.

6.3.2 Recruitment of research participants

The recruitment of research participants within the project raises a number of ethical and legal issues that must be addressed, with specific dimensions arising in relation to internal and external research participants.

The procedures and criteria, as follows, are based on the above-mentioned *Horizon 2020 Programme: Guidance How to complete your ethics self-assessment* and, in particular, section 2.1 (see pp 6-11). Pilot participants will primarily be employees of aqua3S project partners and related organisations. Participation in the pilot for end-user staff may be mandatory as they will be completing training through the company. However, the participation in aqua3S activities (such as evaluations and interviews, etc.) will be voluntary. Given the power asymmetry between employees and supervisors/employers, partners need to ensure that no employee feels compelled to participate in any activity and explain clearly that the employee's job status or privileges are in no way dependent on their participation in the research activity.

The project will not include any children/minors or other persons who are unable to provide lawful consent or vulnerable persons as research participants. All participants in aqua3S activities will be volunteers who have actively consented to participating in the research activity. Their involvement will be required for validation of the developed services. The validation process will be based on synthetic scenarios of emergency situations. Wherever possible, the volunteers will be employees or directly affiliated with the consortium partners.

The aqua3S consortium is committed to complying with ethical principles and applicable international, EU and national law. We will ensure respect for people, for human dignity and fair distribution of the benefits and burden of research. We will protect the values, rights and interests of the research participants. The consortium will obtain the free and fully informed consent of research participants.

When conducting surveys, interviews or workshops where personal information is gathered and stored, we will pay attention to:

- Privacy – The consortium will not collect any biometric data, such as facial recognition, voice and/or gait analysis from the field trial participants except for the purpose of blurring this data to prevent identification (see section 5.4.1). Mainly, we will be interested in the (pseudonymised) views of participants with regard to the utility and user-friendliness of the aqua3S platform.
- Data protection – The consortium will pseudonymise the details of all participants in the trial and will password-protect files and control access to the files.
- Data management – The consortium will ensure that any data processed in the workshops and field trials complies with the project's data management plan.
- The health and safety of participants – Participants will be able to cease participation in the trial of the aqua3S platform and solutions whenever they want. Participants will have regular breaks.

6.3.2.1 Internal

The partners will seek a 50-50 gender balance in the recruitment of employees, preferably with different ethnic, linguistic, geographic and, as far as possible, different professional backgrounds and ranks in the organisations. Such diversity will give researchers a better appreciation of how effective

and user friendly the aqua3S system is. Whenever possible, the project partners will pseudonymise any personal data gathered from the participants during the field trials. Noted exceptions will be photos or videos taken with consent for communication and dissemination purposes. The partners will take every measure to ensure that the recruitment of participants will not involve any discriminatory practice or behaviour, through the following measures. Employees who participate in the field trials will not be given any preferential treatment over other employees who did not participate in the trials. All relevant employees will be given an equal opportunity to receive the training and use of the aqua3S platform and its applications. Further, research participants should be notified of the internal complaints procedures within partner organisations and empowered to submit complaints or concerns if this is the case.

The consortium does not believe that participation in the field trials will incur any psychological, social, legal, economic, environmental or other kind of harm, and will actively safeguard against such harms, for instance by refraining from the use of toxic chemicals and avoiding discriminatory behaviours. Partners will ensure that field trial participants have regular breaks (including lunch breaks) and have an opportunity to express their views at every stage of the field trials. Partners will emphasise to participants that their personal data will be anonymised and/or pseudonymised and protected, that they will have access to their data upon request, that they can withdraw their data and participation at any time up until publication of the results of the field trials.

6.3.2.2 External

Participants will be reminded that their participation is **fully voluntary** and that they can decline to answer to any questions and/or terminate the interview at any time. Where possible, all participants will be asked for their written consent and confirmation that they understand how their data will be used. If requested, participants' identity (including their affiliation) will be pseudonymised, providing them with full confidentiality. This is particularly relevant for members of civil society organisations, or members of vulnerable groups, such as those without formal resident status, who may wish to keep their identity confidential. Participants will have the ability to request that their data be withdrawn at any time during the course of the project. If they so request, the procedures related to the 'right to be forgotten' (described at section 5.3.4).

Partners will interview participants in their native languages (as far as possible) and explain the voluntary nature of the project. During the research, the consortium will ensure that researchers behave in such a manner so as to ensure there is no judgment, discrimination or stigma and that they respect all people they will be involved with interviewing.

All participants will be provided with the details of the project contact points for contact for questions, concerns, or further information – thereby establishing pathways for relaying concerns, as well as the speedy identification of persons to contact for the withdrawal of consent or to request the deletion of information etc.

6.3.3 Notification

Active consent will be sought where possible and practical. However, with some tools, such as the drones and social media crawler, it will be more difficult to proactively request the consent of partners. Where consent is not used as the legitimate basis for processing personal data, other bases will be relied upon, for instance:

- The vital interest of the individual

- The public interest
- Contractual necessity
- Compliance with legal obligations
- Unambiguous consent of the individual
- Legitimate interest of the data controller

Nevertheless, the Consortium will provide notification of the local community at the time of a demonstration (e.g. through social media, the local press and placing notifications at the testing sites) that trial activities will be/are being undertaken in order to better enable the public to exercise their agency, contact the project in case they would like to request specific actions, and help to encourage public trust and awareness. The notification itself should state that the test is part of an exercise and not a genuine emergency. Subsequent notifications and warnings, once the system has been deployed, should state when the notification is part of a real or test emergency exercise.

6.3.4 Data storage and sharing

The aqua3S project has outlined a number of measures related to the GDPR compliant storage of personal data (Deliverable 1.2 – self-assessment and data management plan v.1). These primarily relate to access controls and the physical restriction of information containing personal data.

Nevertheless, under the GDPR, personal data must also be deleted or anonymised once it is no longer required. Additionally, further to the 'right to be forgotten' and the general withdrawal of consent, the party storing the data may be legally obliged to delete personal data in certain circumstances. This requires the positive obligation to have procedures in place to allow this, in compliance with the GDPR in such situations. Further, to comply with Article 17 of the aqua3S grant agreement, after the duration of data process period (five years after the project's last payment) or if the informed consent has been revoked (the sooner applies), all personal and sensitive data will be deleted from the databases of the consortium.

Each end user has a system for collecting and storing personal data which is outlined in deliverable 1.2 'Self-assessment & Data Management Plan V1'.

Recommendation:

Time limits for the storage of personal data should be set in order to retain consistent GDPR compliant behaviours. After the expiration of duration of data process period (five years after the project's last payment) or if the informed consent has been revoked (the sooner applies), all personal and sensitive data will be deleted from the databases of the consortium.

Processes should be established in order to ensure compliance with the right to be forgotten or the withdrawal of consent, where they are not already in place. This may include the review of existing processes, to ensure that such personal data is capable of being deleted, and reviews of automatic processes to delete personal information (such as within the social media crawler), to ensure that they are correctly removing personal data and deleted tweets.

6.4 Concerns identified through the impact assessment & mitigation measures

Each element of the aqua3S core concept can be related to a set of legal, ethical, and social issues which must be negotiated by the aqua3S solution's development and design, as well as by organisations that may later adopt any resulting products. This section highlights keys aspects of the

concept and the related risks that could arise in design and use. Subsequent sections build upon these risks and issues by analysing the interviews of technical partners for information flow, privacy law, and user requirements.

The key issues are outlined below. Though some of issues can be mitigated through system design, a number of issues relevant to the overall high-level concept, technologies, and expected practices, go beyond the scope of what can be addressing during this project. They are included, however, because they represent the larger ethical and societal impacts, beyond the project's demonstrations and exercises. The provided recommendations for these issues include recommendations that will not be actionable within the aqua3S product development but are nevertheless relevant as the issues may arise through the use of the aqua3S system. Any considerations towards them can increase the likelihood of uptake, sustainability, and increase the public good offered by aqua3S.

Within this section *'recommendation for the development of the aqua3S solution'* refers to the functional requirements and actions that should be taken during the aqua3S project. *'Recommendation for future use of the aqua3S solution'* refers to the actions that should be taken by water service providers adopting the aqua3S once it has already been developed. In this respect the latter form of recommendation refers to the post-project stage.

6.4.1 Privacy and personal data infringement

The aqua3S solution involves the collection of information from a variety of sensors (See KR01-03). Though some of this information sources pose little risk to the privacy and personal data of the population (such as the sensors for substance detection), several of the features may potentially do so, as outlined below. The areas of primary concern relate to social media crawling, CCTV and UAV features within the system. The capturing of visual media risks infringing on individuals' privacy rights, as well as their personal data (through the capturing of information that can be used to identify the individual). Though measures (described below) are being incorporated into the aqua3S solution to minimise this risk, there will be a residual risk that personal information will be captured. Further, given the differences in national. regulations governing the use of unmanned aerial vehicles, this may result in confusion over the applicable regulations, potentially leading to subsequent accidental breaches.

These particular tools will be considered individually, in light of the relevant privacy and personal data challenges, in the sub-section below.

6.4.1.1 Social Media Crawler

The Social Media Crawler is described above at section 6.1 (KR03). The Social Media crawling procedure is a JAVA component that constantly runs using Twitter's Streaming API to retrieve tweets according to specified search criteria. When a tweet is collected, three different APIs are called to estimate its validation (real or fake) and its relevancy (relevant to the use cases) and to detect any locations mentioned inside the text. The results of the analysis are added to the JSON structure provided by Twitter with all the information of the tweet and then the JSON is stored to a MongoDB.

For each tweet a JSON that contains all the information provided by Twitter plus the analysis outcomes (verification, relevancy estimation, and localisation) and is stored to a database. The collection of these social media posts has the potential to collect personal information, though they remain in the public domain. However, in adopting a data minimisation approach, the following

approaches are to be taken within the aqua3S to ensure that the unnecessary personal data is collected.

Recommendation for the development of the aqua3S solution:

In order to guarantee the protection of data within the project the following aspects will be implemented with respect to the data gathered through the social media crawler technology:

- The basic approach of the project will be to anonymise all collected data. The acquired data will under no circumstances be used for commercial purposes or shared with any third parties (excluding access by EU and research purposes, under specific guidelines that will be provided by the project). If such datasets (i.e. the collected tweets) will be created, they will be provided for relevant EU personnel and researchers after the end of the project.
- The project will follow the formal procedures that are explicitly defined within each partner organization to protect the anonymity of data that are shared among the consortium.
- Further, social media posts will be screened for relevancy through a list of relevant keywords developed by the consortium. This will limit the unnecessary collection of irrelevant information and the 'over collection' of personal data, even where data is anonymised/pseudonymised.
- Collection in this phase will focus on individual posts and (where available) any response by the water companies. In this phase, we will assume the default position that each post collected is made by an individual and thus may contain personal data. Therefore, both the account name and username will be hashed upon collection and the original data stored separately and securely in a database with key tables to ensure research accountability and integrity.
- Any post that mentions the word house/home/apartment or similar will undergo additional manual redaction to ensure that any personal addresses are not included in any further processing activities.
- aqua3S should not collect the posts of those who have placed privacy restrictions on their account/post.

These recommendations refer to existing aqua3S policies as put forward by CERTH. Therefore, no breaches are expected.

However, the steps outlined above should be disseminated to system users, and efforts should be taken to ensure that these processes are working as intended through the project

6.4.1.2 UAVs (drones)

UAVs (also referred as 'drones') are to be used within the aqua3S module KR02 (Visual content acquisition module). This is outlined in more detail above at section 6.1.

Within the GDPR, any information that allows an individual to be identified constitutes personal data (Article 4). This can include a range of information (images and videos) that can be captured by the drones that are to be deployed within aqua3S (such as faces, vehicle licence places). Nevertheless, the aqua3S drones will not be used to capture audio data. This creates a variety of issues that must be considered when relying on UAV sensors.

The primary concerns relate to the initial capture of data, and secondly the transfer and storage of data after it has been received. The former relates to the technical features of the drone, whilst the latter is more related to the organisational protocols in place to safeguard the contained personal data.

The legislation defines the requirements for drone design and operation to protect the safety and the privacy of EU citizens. It also enables free circulation of drones and common rules within the European Union. Operators are required to register their drones in the Member State where they reside or conduct business; but once given a permit, they can fly their drones across the whole EU.[6] The regulations include technical requirements such as the capabilities a drone must have to be flown safely. They also cover operational rules, distinguishing between operation types, from those not requiring prior authorisation, to those involving certified aircraft and operators. They also define minimum remote pilot training requirements. These requirements should cover the essential requirements provided for in Article 55 of Regulation (EU) 2018/1139, in particular as regards the specific features and functionalities necessary to mitigate risks pertaining to the safety of the flight, privacy, and protection of personal data, security or the environment, arising from the operation of these UAVs. Of specific interests are:

- Article 13(1), Cross-border operations or operations outside the state of registration, regarding the necessary authorizations and documented location and purpose of intended operation,
- risks associated with that operation (in accordance with Article 11(2)(b) specific to the local airspace, terrain and population characteristics and the climatic conditions, and, if necessary, mitigation measures adopted.

While KR02 has such legal requirements in view, there is a small risk that its flight capabilities and data processing interactions with other parts of aqua3S might exacerbate privacy challenges of incidentally gathered data.

Drones will also produce noise in their use. Existing EU regulations (European Commission Delegated Regulation (EU) 2019/945 and European Commission Implementing Regulation (EU) 2019/947) regulate the environmental impact of drones, including a maximum permitted noise level. Nevertheless, the impact and consequences for individuals, wildlife and the environment are not fully known. It remains possible that the noise emitted by the drone system will produce negative impacts in these areas, including the water system (Christiansen et al. 2016). The EU Aviation Safety Agency (EASA) is currently working on a draft opinion on a U-space regulatory framework which aims to address such issues.

Recommendation for the development of the aqua3S solution:

Ensure that any aqua3S user wanting to engage with the drone module has received the necessary training in local laws in order to comply with relevant regulation when he designs the flight paths. This training would be equally valuable for preparedness training (learning how to use drones in ways that are least privacy infringing, even in emergency situations) and response (outside of aqua3S' current view, but part of what training points to). The EU project 'Drone Rules' and 'Drone Rules Pro' have

[6] https://dronerules.eu/en/professional/news/easa-eu-wide-rules-on-drones-published

provided detailed support for both identifying the privacy and security risks of drone use, as well as guidance for drone privacy-by-design. Keeping these resources prevalent while final aqua3S design decisions are made will help ensure regulatory compliance. The documentation can be found here:

- https://dronerules.eu/assets/files/DRPRO_Privacy_by_Design_Guide_EN.pdf
- http://dronerules.eu/assets/files/PCC_DR_final-for-printing_9-November-2018.pdf
- http://dronerules.eu/assets/files/DPIA.pdf

Manual and automatic flight scenarios should be deployed with professional and certificated drone pilots. Where a user does not have an accredited drone operator internally, an external accredited drone operator should be used for the purpose of the pilot. Moreover programmed drones with state-of-the-art flight technology to be recruited and designed for these purposes. The certification should be sought from the relevant national authority for civil aviation. Moreover, local insurance should be obtained. The recruitment of a trained professional and the use of state-of-the-art flight technology should be used to ensure that the UAVs capture as little data on uninvolved/non-consenting adults as possible. With regard to video data collected by UAVs, personal data such as faces, and licence plate numbers will be automatically blurred.

The aqua3S consortium will also try to plan the flight routes during the pilots to minimise the chance of capturing personal data. In doing so, the flight plan can avoid urban areas and seek to minimise the impacts of noise pollution on the local environment. It is important to note that due to the limited battery capacity of the drone, the drone flight domain will be relatively restricted, and impacts will be for a short period of time.

Data retention policies should be in place, so that the stored personal data can be deleted once it is no longer necessary.

The drones used within the aqua3S must meet the regulations set out in Commission Delegated Regulation (EU) 2019/945 in relation to sound that they produce. Moreover, in selecting the UAVs used for the project, the sound of the drone should be taken into account as a relevant consideration. During the project pilots, efforts should be taken to assess any negative impact on humans and the natural environment, with questions related to this issue captured within questionnaires.

Recommendation for future use of the aqua3S solution:

The recommendations and processes outlined above should be implemented within the water service provider's processes and procedures.

6.4.1.3 CCTV

CERTH will commence research on the use of CCTV in the second year of the project and specifically after M14 (where CERTH have the first versions of the deliverable for T3.2 'Area monitoring using UAVs and satellite data' which will involve the collection of data from UAVs and CCTVs). This research will also be dependent on the interest of EYATH in using such sources. Further research will be conducted as our knowledge of this tool develops in future.

Recommendation for the development of the aqua3S solution:

With regard to video data collected by CCTV, personal data such as faces, and license plate numbers should be automatically blurred. Additionally, attention should be paid to the placement of these components, in order to seek the least intrusive means possible, i.e. placed in such a way that they avoids capturing personal data, or seeks to minimise such intrusion.

6.4.2 Ethical challenges posed by cyber-attacks

6.4.2.1 Societal vulnerability

The use of remote sensor systems can potentially create pathways for cyber-attacks. In this respect, the IoT processes used within the aqua3S solution can allow water infrastructure to be remotely infiltrated. In extreme cases, where there access to the SCADA is unrestricted and there are no manual controls, cyber-attacks can result in kinetic effects on critical features of water services. Weak security systems may be then circumvented, allowing infiltrators to manipulate flood gates, interfere with chemical and water levels, and even divert irrigated water. Moreover, in such weakly protected systems, where customer information is contained in water systems (i.e. the type necessary to get the water from plant to house) it can be remotely retrieved, posing a concern for the privacy rights of service users. A distinct set of threats may appear in contrast to the usual anticipated harms of lack of water provision.

As technological innovation is frequently built into existing legacy systems, it is necessary to ensure that retrofitting innovation does not ignore the concern that legacy systems may include due outdated components vulnerable to infiltration. Where unpatched code remains, innovation measures must seek to actively address and overcome these challenges (Adepu, et al. 2019).

SCADA systems, which integrate old and new technologies, - industrial business systems and the IoT-cloud system , become more susceptible to infiltration than the traditional, less advanced SCADA systems (Said et al.: 2016). Whilst recognising the advantages that IoT connected systems may bring, they may also bring a number of vulnerabilities. These include: configuration errors from default factory settings, vulnerability in cloud services, memory corruption and weakness in validating input data, and ultimately the vulnerability of system commands and information to interference (Said et al. 2016) Furthermore, there is the potential that infiltrators will be able to retrieve sensor data (by hacking the SCADA system), providing them with the ability to divulge restricted data such as data on water quality and quantity.

The cumulative result of these vulnerabilities are that the combined integrated systems are at risk of advanced persistent threats, such as: the lack of data integrity where data is destroyed; man-in the middle attacks where the attackers gained illegitimate access or monitors the messages and activities within the system; replay attacks which delay messages sent to physical devices and denial of service attacks which prevents the system from performing tasks by overloading the computer resources (Said et al. 2016).

Additionally, given that information on a number of separate areas is contained within the aqua3S system, one of the ways to ensure security is to limit information to those who specifically require it. For example, access restrictions across each theme of information should be considered, particularly when sharing information with first responders, to limit the level of divulged information to align with necessity. Importantly, this concern relates to the future commercial use of the system, as such sharing will not take place in the project pilots themselves.

Security measures are being developed within the aqua3S project by security expert partner BDI. However, given the evolving sophistication of cyber-attacks and the room for human error, it is impossible to discount the potential for any cyber-attack (no matter how small such a risk might be).

Recommendation for the development of the aqua3S solution:

A proportionality assessment should be conducted when determining whether to implement the

aqua3S solution within their system on whether the risk of cyber-attack outweighs the advantages for water security gained by the aqua3S system. As part of the efforts to technically and organisationally secure the aqua3S system from infiltration, the new vulnerabilities that arise from the new avenues for cyber-attack should be considered. This should include an assessment of issues such as the geo-political dynamics that relate to cyber-attacks and the resultant likelihood of cyber-attack, the potential kinetic and digital effects of cyber-attacks (including the effects on individuals as well as other services and infrastructure reliant upon the water sector, such as energy production), and whether the aqua3S system ultimately exacerbates the risks of negative impacts.

Additionally, training should be provided to all relevant personnel on cybersecurity, and means to detect, prevent and mitigate cyber-attacks.

The standard for the project should be that the cyber-security of the water network should be at least equal, but preferably above, to current standards.

Recommendation for future use of the aqua3S solution:

The recommendations outlined above should be implemented within the water service provider's processes and procedures.

6.4.2.2 Societal harms of misinformation on social media

Social media engagement has very low entry costs for users, in terms of access to technology, ease of use, and advances in artificial intelligence. Therefore, the generation of fake media is increasingly feasible (Qawasmeh, et al 2019, p.383-4). Nevertheless, where social media posts are used to determine positive action, it is possible that state and non-state actors could manipulate responses by fabricating instances of water security.

Though measures are being developed within the system to identify suspicious posts generated by 'bots' (i.e. through volume of posts on water security). However, sophisticated attempts may be able to evade such measures. Particularly where a single post can be viewed as warranting a response, the ability to manually create a fake post (thereby avoiding the automated tendencies that make fake posts easier to detect) can be easily achieved. The resultant concern will be that this will result in societal harm or a wasteful use of resources to verify fabricated reports of water security on social media.

Additionally, the perception that social media posts designed to trick the system are a threat may undermine trust (including public trust) of the system, due to vulnerability to such concerns.

Recommendation for the development of the aqua3S solution:

Training should be provided to systems users on the potential for fake social media posts, in order to foster awareness, as well as the recognition that efforts must be taken to verify this information, as opposed to reacting purely on the basis of their existence. The information gained through the social media crawler should be triangulated with other sources in order to verify the information.

During the pilot stage, the time taken to verify the information gathered from social media should be recorded to assess whether this process could become a burden on time and resources. Moreover, should it be necessary to create synthetic tweets about possible threats for the purpose of the pilot, the fact that this information is incorrect and direction to additional information of the aqua3S project should be included in the tweet itself in order to avoid the spread of misinformation.

Recommendation for future use of the aqua3S solution:

The training outlined above should be extended to staff within the water service provider.

Additionally, the measures that are going to be developed to mitigate the threat of fake social media posts should be implemented and reviewed on a periodic basis, in order to keep abreast of developments in strategies of fake media dissemination.

6.4.3 Risks and Issues in crisis communication

6.4.3.1 Insufficient reach of crisis communication

Water service users (whether formal or informal) come from a vast array of demographics, differing in terms of class, gender, linguistic groups, residence, disability to name a few. As these demographics influence their access to information systems, different forms of communication (through choice of medium or language) may be necessary to reach communities.

The concern remains that failing to reach certain communities may privilege members of more affluent, younger and urban populations (who are more likely to have access to technology and use social media), as well as those who speak the language that is used to communicate the message. The result is that those who are less likely to use social media (such as those without mobile phone access maybe be excluded as a result. (Deloitte 2017, p.2)

Computer ownership across Europe is now widespread (with nine Europeans in ten owning a computer). However, there are considerable social determinants on access to digital technology. For instance, working-class communities are less likely to have a computer; geographic location also having a bearing (e.g. usage is lower in central and eastern Europe as well as Portugal). Similarly, under half of working-class populations in Europe know how to use the internet, compared to three quarters and four-fifths of the middle and dominant class respectively. Farmers, cleaners, farm labourers, manual labourers and skilled workers in craft or the food and drink industry, as well as construction, reported experiencing the greatest difficulty in the use of new technology. There is also a gender divergence amongst working class technology users, with an eight percent difference in the grasp of technology. In regard to age, 70 percent of people between 25 and 35 have a good grasp of information technology and 32 percent of those aged 50 and over (Penissat, et al. 2020, pp.47-9).

The communities who are less affluent or do not speak the language of the communication (likely a linguistic minority group) may also be particularly vulnerable. As such, they may have a lower level of resilience in the face of water insecurity and therefore may require the most targeted attention.

However, it is important to note that this presents a distinct ethics opportunity, as it will allow the dissemination of warning messages to those who do not use/use less frequently traditional media such as televisions or home telephones. As such tendencies are increasing, it will allow for the further reach of warning messages.

Recommendation for the development of the aqua3S solution:

Efforts should be made to gather information on the various linguistic groups within the concerned areas, as well as their use and access of communication systems across various demographics. For instance, this should include information disaggregated to include the protected characteristics for non-discrimination purposes where such information is available.

The social media platforms used to disseminate warning messages should give preference to platforms

which have a user-base that is more representative of the general public, for instance Facebook.

Recommendation for future use of the aqua3S solution:

In the long-term, consultation with the public may be conducted in order to understand their needs in regard to messaging, in order to accommodate this into planning.

Attempts should also be made to utilise a variety of communication systems in order to ensure that the messaging is adequate, i.e. through social media, mobile telephone services or local announcements.

6.4.3.2 Counter-productive warning messaging

Both KR14 and KR15 involve the development of warning messaging to disseminate to citizens in times of an emergent or ongoing emergency. In doing so, CERTH will gather social media data from open and public Facebook and Twitter accounts and pages and, in the case of KR15, reinforcing this with desk top research. The output of these tasks is the development of guidelines and plans, aimed at validating incoming information for situational awareness and communicating with citizens (KR14) and the development of language agnostic messages that will be used to communicate automatically with communities upon the detection of an event by the aqua3S sensor network (KR15)

Water insecurity will affect different communities in different ways. The provided information will have a bearing on resultant behaviours. Nevertheless, the challenge remains as to whether it is better to merely provide information on the nature of the water insecurity situation, or whether one should provide information or to attempt to provide information on how they should respond in order to avoid harm. However, where specific guidance is provided, it will need to be tailored to the capabilities and resilience levels of the affected or potentially affected population. Should advice be provided in such a manner that it is not realistic for the population to action, it may ultimately be counter-productive where the guidance is not suited to their context.

Early warning systems (EWS) are considered 'vital infrastructure for society' (Baudoin 2016). EWS can help to empower communities and vulnerable groups by ensuring that they have the necessary information to cope with insecurity. In this sense, we can recognise EWS as tied to the population's resilience. However, adopting participatory EWS measures that are ultimately tailored to the context and perspectives of the concerned communities (Baudoin 2016) can act to bolster the expert-led measures by including community voices within the messaging.

Community-centric EWS have been proffered as one such method to achieve this (Baudoin 2016). Indeed, the aqua3S system includes such processes within its solutions, by collecting citizen generated information on social media (as discussed above). However, the dissemination of warning messages among at-risk groups, and the facilitation of the implementation of emergency plans or responses that can allow communities to best mitigate the impacts of water insecurity is less articulated within the aqua3S system. This will ultimately relate to the selection of appropriate communication channels to disseminate warnings in a manner that allows community members to 'contribute to increasing the engagement of the beneficiaries.'

Udu-gama (2009) underlines how using appropriate communication channels to disseminate warnings that are accessible and relevant to community members can contribute to increasing the engagement of the beneficiaries. This can help to increase societal ownership as well as the effectiveness of the EWS itself.

The development of community centric EWS implies a recognition that communities will have distinct levels of resilience, will face different threats in coping with insecurity and will have varying abilities to engage with EWS depending on their demographic characteristics (for instance, across the gender spectrum, for persons with disabilities and socio-economically disadvantaged communities). Where the EWS does not include a recognition of these particularities, they may contribute to inequality by 'increasing the marginalisation and vulnerability of groups who have less power and influence' (Brown et. al 2019, p.1). This has important repercussions on the development of EWS measures, which may need to involve proactive measures to capture the particularities of marginalised, in order to ensure that their voices are heard within EWS processes (Brown et al. 2019, p.1). This may be due to the fact that marginalised groups may be less able to participate in EWS initiatives, for instance, due to mobility changes or work-based limitations. This will also have a strong bearing on the issues that are relayed in EWS. As exemplified by Brown et al, the threats that communities face are recognised and prioritised differently across the gender spectrum. To identify the pertinent threats to communities, specifically tailoring our understanding of threats to these community groups is an important step.

Additionally, access to early warning will also differ across demographic characteristics. For instance, economic capital, access to technology and social capital, can influence the ability to access or to act on early warning communications. As such, an intersectional understanding of community groups is required to appreciate the obstacles they face with regard to EWS and the resultant responses.

Recommendation for the development of the aqua3S solution:

Warnings should be tailored to the capacities of the target audience. In doing so, the warnings should avoid adopting a 'one-size-fits-all' approach, and instead provide individuals with the ability to effectively act on the information provided (in terms of recommendations on suggested behaviour in a manner suited to their context, etc.). Should this information not be contained within the message itself, the message should direct the public to more specific recommendations on how to respond in a manner that takes specific vulnerabilities into account.

In order to achieve this, in developing the warning communications, community consultation (regarding their vulnerabilities to water insecurity, preferred communication channels and useful advice) should be conducted.

Ultimately, an intersectional lens should be used in developing communication strategies, in order to account for the particular vulnerabilities and contexts of various demographics.

6.4.3.3 Insufficient information for response prioritization

The Crisis Classification (CRCL) (KR13) is outlined above at section 6.1. The information that is captured and provided to aqua3S users will ultimately be used to inform responses. Nevertheless, as the reported harms relate to the water network and quality itself, this does not contain sufficient reference to how these harms will manifest in relation to the human population and wider environment. The particularities of human and environmental vulnerability will be necessary to determine response prioritisation.

As outlined within the literature and international legal instruments and guidance, certain demographics are at particular risk of harm resulting from water insecurity. This therefore points to a need to develop an intersectional understanding of human vulnerability to inform response measures, and as well as the need to avoid the development of a 'human-agnostic' system, that presents 'harm', as harm to the water network or water quality without appreciating how these ultimately impact communities.

Where a limited selection of information is provided to systems-users, it may provide the illusion that it is an exhaustive collation of the necessary information. However, response measures should be tailored to the contexts in which they arise. A system that does not contain information on the vulnerability of the human or environmental conditions may foster decisions that are tailored to the integrity of the water network, and, in doing so, pay insufficient attention to the intersectional impacts of water insecurity resulting in one-size-fits-all responses.

Automation in some ways is counter to the unforeseen nature of disaster. One reason why disasters happen, is because they affect societies in unexpected ways, that defy all preparedness measures and resilience infrastructures. Automation can pose a challenge for the adaptability necessary for system resilience.

Recommendation for the development of the aqua3S solution:

The crisis classification system should seek to also factor in the vulnerability of the population. Such information should aim to include information on the population density, the socio-economic dynamics of the population, demographic characteristics and their relation to vulnerability to water insecurity. The demographic analysis should aim to include information on the following groups, identified within human rights law instruments and guidance on the right to water:

- women,
- children,
- minority groups,
- indigenous peoples,
- refugees,
- asylum-seekers,
- internally displaced persons,
- migrant workers,
- prisoners and detainees,
- persons with disabilities

The calculation of crisis should avoid a 'human-agnostic' approach, it should recognise instead that the severity of a crisis is inherently linked to human and environmental vulnerability. The response measures should therefore give priority to those who are particularly exposed to harm.

Notably, this information should not be on an individual level, but rather, the aggregated characteristics or a particular demographic. Where unavailable internally, this information should be gathered from municipal authorities.

Where this information cannot be included, the system should highlight to the user that information on human vulnerability and resilience will be necessary factors in determining responses and direct the system user/decision-maker to include human resilience and vulnerability in the decision-making process.

During the pilot stages, efforts should be taken to assess how human vulnerability is filtered into the decision making and prioritisation process. Information regarding these vulnerabilities should be easily accessible and it should be placed particular attention on vulnerable demographics and key sites and infrastructure (i.e. hospitals).

6.4.4 Risks and issues in automation

6.4.4.1 Automation Bias in Decision Support Tools

Decision support mechanisms are to be utilised within the aqua3S in relation to KR08 and the development crisis management approaches. Though this helps to assist decision-makers through the provision of information that may otherwise be difficult to ascertain, there is potential that it will promote behaviours that are affected by automated suggestions. This may be as a result of undue deference to the automated decision or conversely, undue hesitancy to rely on an automated decision. This concern ultimately relates to the concept of automation bias.

Automation bias is the phenomenon where human agents are unduly deferential to automated decisions or guidance. Some studies have demonstrated that those using automated systems place greater trust in the automated decisions than their own, even where their own judgment and experience may have otherwise led to a different decision (Keats Citron: 2008, 1271 & nn.147-8). This perhaps arises from the belief that automated decisions result from 'indisputable hard science, or that they operate at a level beyond human capacity' (Deeks et al. 2019, p.17). Additionally, it remains possible that system-users are still hesitant that they may be held responsible for ensuing harms when overruling the automated decision, and that following the automated decision mitigates culpability. As reported by end-users, it is also possible that decision-makers will distrust the results from entirely automated processes. Where such tools are deemed to be unreliable or incorrect, it may cause the decision-maker to rely on human intuition and experience with less reliance on objective information.

Automation bias in decision support mechanisms provides an ethical risk in relation to the aqua3S project as it may inhibit the decision-making role of system users. This can ultimately limit the contribution of expertise and domain knowledge held by system operators. Moreover, human operators may able to consider and balance a range of issues that may be outside the scope of the system when determining an appropriate response. Deference to automated decisions or recommendations may therefore limit the scope of a response to only those factors that are built into the automated system.

Recommendation for the development of the aqua3S solution:

During project pilots, participants using the system should be asked to provide feedback on whether the system influenced their decision-making process and particularly, whether they felt directed towards a certain conclusion. Additionally, the same participants should be asked about their perception of the quality of the information being provided (i.e. the degree to which they trust the represented information and the extent to which they feel that additional checks are required).

The Decision Support Mechanism should highlight that other information will be required to make a decision, in order to highlight that the platform is not the ultimate decision-maker but is merely to provide information that is to be utilised by the human decision-maker.

The information that is relied upon by the system should be displayed to the user, thereby allowing users to identify where there may be a gap in the analysis or where additional information should be sought.

Training should be provided to the users of the system to explain the concept of automation bias in an accessible and understandable manner. This training should also seek to outline accountability processes within the organisation, as well as contact points for seeking additional information. In order to foster trust in the systems themselves, it will be important to communicate the nature of the tool

(its functions and limitations) and remain open and transparent about issues such as accuracy.

Recommendation for future use of the aqua3S solution:

The training outlined above should be extended to staff within the water service provider.

6.4.4.2 Indirect bias in data collection and system responses processes

Within the aqua3S solution, information is gathered from a range of sources and used to inform water security responses. One possible side effect is that this information may be gathered in such a way that it brings more information from specific demographics.

For instance, in regard to social media crawling, social media users tend to come from more affluent and urban groupings. Technologically, where the crawling measures are only able to capture references to water insecurity in specific languages, it will give a preference to information provided by certain linguistic groups. Where this information is used to inform responses, a failure to weigh the disproportionate level of information from certain demographics may mean that there is indirect discrimination against those who do not benefit from the same privileges.

For example, within the UK, Twitter users (the source of posts for the social media crawler) made up a small percentage of the population (18.6% in 2017) and were ultimately unrepresentative of the population. Twitter users were more likely to be younger, male, have a tertiary level of education, be politically engaged and support left-wing political parties than the general public. (Mellon, J., & Prosser, C. 2017).

This concern also exists in relation to satellite imagery and UAVs. Some water security issues such as pollution may be more visible in open environments than closed urban environments. It is therefore important to consider how intrinsic physical limitations of the technology can contribute to indirect bias.

The core of this concern is that decision-makers may fail to appreciate that information will be captured in an uneven manner that preferences certain demographics; where this is not weighted sufficiently, will result in indirectly discriminatory responses and prioritisation.

Recommendation for the development of the aqua3S solution:

In recognising that non-discrimination is enshrined within the right to water, there is a need to ensure that efforts are made to avoid paying disproportionate attention to the needs of particular communities, where this attention is not warranted by the vulnerability of this community.

Efforts should be made to ensure that a disproportionate weight is not given to information that is collected from social media. In doing so, training should be given to system users to highlight these issues, and the need to seek information from other sources.

The information that is gathered through the social media crawler should not be treated as the sole source of information for decision-making, but additional information should also be sourced from areas (such as call centres, or sensors) where feasible. aqua3S must emphasise its focus on sensors as the primary sources, with sources such as social media posts acting to enrich this information

Recommendation for future use of the aqua3S solution:

The other sources of information that are to be used in tandem for the collection of information on anomalies in water networks should be deployed in such a way that the system is able to capture information from communities who are less likely to use social media. For instance, more

impoverished areas should be directly addressed. For the future use of the aqua3S system beyond the scope of the project, this will mean careful consideration in the placement of any sensors in the water network and the advertisement of existing call centre contact and procedure information in such areas.

For the future use of the aqua3S system beyond the scope of the project, specific efforts may be needed to perform outreach activities to obtain the insights from less accessible communities (such as irregular migrants). This may include providing such information in multiple languages where there is a sizeable linguistic minority population. However, within the product development stage, this is restricted to the primary languages of the end-user's countries as well as English.

6.4.5 Resource risks and issues

6.4.5.1 Requirement for system maintenance and upkeep

The aqua3S solution is fed by the data that it collects from a variety of sensors. Where these sensors are compromised, the aqua3S solution will be less able to respond to water security threats. Should the aqua3S solution be adopted by water service providers following the aqua3S project, the aqua3S sensors will require regular monitoring of functionality, maintenance and potentially updating the sensors and system to ensure their integrity.

The resources used to ensure these issues may be disproportionate, particularly where the sensor system is extensive. A lack of resources in future may mean that responsible bodies will be unable or unwilling to invest sufficient funds into these efforts, creating a reliance on an ultimately flawed sensor system.

The ethical concern that remains is whether the initial investment needed to implement the aqua3S solution in the first instance detracts resources from funding in other areas. Subsequent restrictions in budget may then lead to a situation where the aqua3S is not able to provide its solutions effectively, whilst the wider capabilities have received less funding, and are therefore less able to fill the protection gap that has been created.

Additionally, it will be important to ensure that human personnel remain able to provide support and to provide human oversight over the automated aspects of the aqua3S solution. This will mean that there will be investment costs for the aqua3S solution, as well as in the continued development of the skills and knowledge of water network personnel. Failing to do so, may mean the underdevelopment of skills and knowledge in a manner that reduces future capacity to respond to harms. An example of this relates to machine learning which can lead to the underdevelopment of skills and knowledge (e.g. smartphone maps resulted in a reduction in the ability to read maps) (European Political Strategy Centre 2018).

Beyond the immediate threat of cyber-attacks, there is also a resource burden arising from the need to protect the system against cyber-threats. For instance, staff will require training to sensitise them to threats and responses, as well as the costs related to updating technological equipment throughout their lifecycle to safeguard the system against cyber-attacks.

Moreover, despite the increasing frequency of cyber-attacks on water networks, the concept remains relatively novel, particularly within the European context. As such, where remote sensing is utilised within the system, the potential for cyber-attacks may not receive adequate attention or investment. In this sense, where the resources are scarce in the first instance, water service providers may be

hesitant to invest the necessary funds to safeguard against a vague hypothetical and potentially unrealised threats. As a result, the security concerns must be appreciated by senior staff, or those with decision and investment-making positions, in order to ensure that they are aware of the seriousness of these threats (Germano: 2018).

As sensors bring geopolitics into view, the needs for more resources shift towards cyber security (away, likely from more marginalised social needs), and focuses water security as an infrastructure problem. Yet, invisible toxicities bring into focus how living conditions and structural inequalities in society, even in wealthy nations, still drive less tangible and democratic water insecurities, vulnerabilities only partially addressed through sensors.

This may result in the redrawing of resource prioritisation. Particularly as national security concerns are intertwined with water security considerations, attention must be paid to ensure that the population is protected alongside key governmental institutions.

Interconnected water networks require a raft of cyber-security measures. These measures continue along the life-cycle of the use of the system and may entail the provision of cyber-security training to staff and the updating of security systems. As governments become increasingly focused on the risk of cyber-attacks, there may be a drive to prioritise cyber-security capabilities.

Recommendation for future use of the aqua3S solution:

With regard to the future use of the aqua3S system, beyond the scope of the immediate project, awareness for the need to engage in ongoing maintenance, updating and training should be taken into consideration when determining budget allocation, and initial investment. The provision of such activities should be deemed as essential to the aqua3S solution, that is required alongside the immediate investment in the aqua3S system itself.

Moreover, the importance of the right to water should be recognised throughout any decision related to cyber-security, and should be respected, protected and fulfilled as far as possible.

Following from discussions with end-users during the ethics workshop, the ongoing maintenance costs are not expected to be particularly high. However, the resources expended on training should be monitored and expended.

6.4.6 Public trust and perceptions

6.4.6.1 Distrust of aqua3S system

With emergent and novel technologies (and particularly in the case of surveillance technology) there is more potential for public concern and distrust.

The use of UAVs, satellite imagery, social media crawling may lead to public concern that the aqua3S system will also be used to establish criminal culpability. These concerns may go beyond fears of criminal culpability, as individuals and communities may perceive them as adverse impacts on their privacy, or the spread of conspiracy theories. Societies and communities may be disconcerted by the regular collection of visual data, particularly where they are unaware of their purpose and may attribute it to other motivations, such as deliberate surveillance of human behaviours. These concerns have been present throughout the context of smart city policies generally (see e.g. Ashton 2019).

Moreover, regarding the use of social media, individuals may be willing to discuss the condition of their water supply, but would be hesitant to do so if they believed that their social media posts would

result positive action by third parties. This may result in a 'chilling effect' on the freedom of expression.

However, in some circumstances, suspicion may remain even where unwarranted. Nevertheless, attempts should be made to minimise these concerns where possible. Importantly, participatory measures (including within smart city policies) have been noted as improving civilian trust of the government and on issues such as general transparency (Webster & Leleux, 2019).

Recommendation for the development of the aqua3S solution:

Efforts should be made to highlight the publicly available information on the aqua3S project (for example, the project website). Information about the tools should be included, and it should highlight the measures that will be taken to better respect privacy. Furthermore, the overall objectives of the project and aqua3S system.

The public should be notified prior to demonstrations, explaining to it the system, as well as information such as the tools that may cause public distrust. However, in doing so, information should also be provided on the measures that will be taken to minimise infringements on people's rights, as well as providing contact points should they have any queries or concerns.

Clear communication with the public and transparency will be integral to achieving this. Further this trust will be enhanced by compliance with regulations and the establishment of a rights respecting and privacy-by-design model within the project to ensure that harms do not materialise. In this sense, it will remain important to highlight the actions that the project is doing to minimise potential harms as well as emphasising the overall objective of the project.

All efforts communicate with the public should be realised with accessible language (i.e. it should simple, concise, legible and should be in multiple languages where there is a sizeable linguistic minority population).

Recommendation for future use of the aqua3S solution:

The recommendations outlined above should be implemented within the water service provider's processes and procedures. This should be done prior to the use of the system, with publicly available information on the system contained on the provider's public facing communication, such as their website and brochures where relevant.

6.4.6.2 Responsible use of the automation in the aqua3S system

One of the functions of the aqua3S solution is to improve efficiency within water services. The resultantly efficiency can be used to minimise costs. However, the concern remains if the advantages of the minimised costs are used for the improvement of general societal wellbeing.

As highlighted by the former Special Rapporteur on Extreme Poverty and Human Rights, Philip Alston, the 'profit motive' incentivises organisations to 'minimise the time spent with clients, close cases earlier, generate additional fees where possible and cater to those better-off with easier problems, further marginalising those with fewer resources or more complex and expensive problems.' (Alston 2018, para.34)

Where the profits are used instead to pay dividends as opposed to investment in infrastructure, this fails to maximise the societal benefit gained greater efficiency.

Service users and the wider community should be viewed as 'rights-holders' as opposed to merely 'clients'. Within international human rights law, states are obliged to contribute maximum available

resources to the right to the economic, social and cultural rights, as outlined in the International Covenant on Economic, Social and Cultural Rights (ICESCR) (CESCR General Comment 3, (14 December 1990, para. 10) . It would appear best practice to ensure (within both the public and private sector) that the resources acquired due to increased efficiency are reinvested within the water sector.

Given the fact that increased efficiency may mean that less human manpower is required, the possibility remains that some tasks will no longer need to be completed by human agents, as well as the possibility that this will exist as a looming concern amongst water service staff, fearing being laid-off in future as a result.

Recommendation for future use of the aqua3S solution:

The expected resource efficiency benefits that arise from the use of the aqua3S should not merely result in increased dividends to shareholders or salary increases for executive staff. Rather, they should be reinvested into the services.

Moreover, should there be an increase in costs in order to implement, maintain or utilise the system, these costs of such should aim to achieve this without placing additional burdens on those less able to afford an increase. Additionally, where resource allocation means that resources must be redirected from other areas, so it should be avoided reducing revenues from activities that are essential for the most vulnerable.

Where the adoption of the system has an impact, or is expected to have an impact on the employment of staff, end-users should engage with staff and representative bodies (such as trade unions) to ensure that staffs' concerns are taken into account, and that they have the ability to make representations.

6.4.7 Data sharing

As data gets shared across different organisational and cultural risk assessment regimes, there is a risk of function creep, where data gathered for one purpose gets used for another. Many disaster response agencies lack the technological skills and capacities to ensure data is accurate, credible, and not mis-leading for those they are sharing it with (Campo et al. 2018).

New trans-boundary risks emerge where data access and limits in data's physical ability to cross a border becomes criteria for hazard and risk reduction.

Data interoperability creates new opportunities for data access. However, having access also creates new challenges for accountability and liability. If someone has access to the data, do they need to respond to it? Will the person sharing the data be held accountable if they did not foresee a risk?

Increasing sources of data can often lead to information overload and compound the challenge of knowing what data to trust.

Property rights issues can limit cross-border data exchange. This can be exacerbated by the different national regulations on this account throughout the EU (Maurer, Firestone, & Scriver 2000).

6.5 Risks and Issues raised at end-user workshop

This section identifies issues raised directly from collaborative sessions held within the ethics workshop in which participants were asked to identify ethics and legal risks and opportunities. The full table of risks and issues raised during the ethics workshop collaborative session is located in Annex A within this deliverable. A summary of the issues is found below:

- Noise pollution resulting from the use of UAVs
- Malign cyber infiltration of water network systems causing kinetic effects and information access (kinetic effects include manipulating water pumps, disinfectant levels, information relating to sewage levels)
- Erosion of societal trust resulting from negative perceptions and insufficient information about the aqua3S system and objectives
- Indirect discrimination resulting from insufficient information collected on/ disseminated to groups who do not use social media
- Automation bias affecting the decision-making process of system users
- Lack of ability to use aqua3S and legacy systems together resulting in a 'double interface' that is difficult to use in an efficient manner, thereby reducing resource efficiency

As these concerns were raised in the recent past, they have been researched and included within this deliverable to the extent possible. However, these concerns will be discussed with partners and included in greater detail in the next iteration of the report (with a final outline in deliverable D2.5 'final ethics and legal framework').

6.6 Legislative compliance in the pilot locations

No barriers to legal compliance in the training exercise and demonstration locations have been identified at this stage of the project. The internal preliminary guide 'Introduction to Legal and Ethical Principles' provides an initial assessment of relevant European legislation. This list will be further expanded as the exercise and technology details are solidified and reported in D2.5 (final ethics and legal framework).

Prior to the pilots, a review will be conducted on the national legislation and guidance to ensure that the pilots abide by the law. TRI will conduct a survey with the relevant end-users to collect information on the applicable national law (for instance, on issues such as drone regulations, public notification procedures, privacy standards) and produce guidelines for the end-user partners and project as a whole.

6.6.1 UAV legislation compliance

European Commission Delegated Regulation (EU) 2019/945 set out rules for the safe and secure use of drones, while the European Commission Implementing Regulation (EU) 2019/947, sets out rules for the design and manufacture of drones. Drone regulations vary by country and region. These need to be addressed and accommodated for in a way that does not merely assume that the lowest common denominator is the solution – i.e. that the least restrictive regulatory system- is to be complied with over the more stringent regulatory regimes.

In Europe, professional drone operators flying over the territory of an EU Member State must comply with Regulation (EC) 785/2004 on insurance requirements for Air Carriers and Aircraft Operators. Article 4 holds that 'Aircraft operators […] shall be insured in accordance with this Regulation as regards their aviation-specific liability in respect of […] third parties.'

7. Preliminary Ethics & Legal Framework

Ultimately, the themes that arise out of the impact assessment can be placed under a number of categories.

At a high level these relate to:

- Privacy and personal data infringement
- Ethical challenges posed by cyber-attacks
- Risks and Issues in Early Warning Systems
- Risks and issues in automation
- Resource risks and issues
- Public trust and perceptions
- Legislative compliance in the pilot locations

Though high-level recommendations have been inserted above under each of the identified risks recommendations, it is possible to distil a number of core approaches that should be embedded within the aqua3S project, as well as within future attempts to take it forward.

7.1 Personal Data

7.1.1 Data minimisation & anonymisation/pseudonymisation

In order to limit any potential impacts to privacy, organisational and technical processes should be put in place to restrict the information held to solely what is necessary within the aqua3S system. Any information that is in fact necessary should be processed only where there is a legitimate basis, and ideally with the explicit informed consent of the data subject.

Minimum data that is necessary for the purposes of the processing should be collected. The data retention period should be five years after the project's last payment or once the informed consent has been revoked where it is the legitimate basis for data processing (the sooner applies). After this period all personal and sensitive data will be deleted from the databases of the consortium.

Along with this, appropriate deletion or anonymisation protocols (such as the one defined for aqua3S in D11.5 – see Annex B) should be designed. Identifying the characteristics of the information that will foreseeably be collected is useful to detect the potential disproportionate collection of data and to minimise it. For this reason, it is necessary for designers and end users to understand the main goals of the system, so that only proportional data processing will occur in the fulfilment of these goals.

Clear and sound definition of the purpose for collection of data must be communicated to the users prior to the moment of introducing any personal data. The collected raw personal data is not a repository that the data processors are allowed to use at their own discretion. The actual utilisation of data has to be justified and made according to the goals of the designed system.

Keeping to the minimal personal data necessary for the purpose will also help alleviate issues around data aggregation and reidentification of persons. For example, end-users could inadvertently recover identities or find additional information about data subjects by clustering data from different sources (Narayanan and Shmatikov 2010). Moreover, claims to anonymity are always relational, defined in relation to security issues at hand (Nelson 2011). It is up to the data controllers to determine when such risks might be necessary and accountable; the GDPR does not provide clear lines on this as proper response depends on the specifics of the situation. Furthermore, unnecessary use of certain

formats can lead to personal data risks: image and video may reveal additional contextual information or accidentally collect, highlight and/or reveal sensitive data.

Anonymisation is a complex problem, with no single solution. Petersen et al. (2017)'s study of anonymisation use in emergency response data systems revealed that anonymising information can lead both to greater trust or less trust depending on prior relations and other aggregated data. It can also lead to more security if in a situation of persecution, or less security if it means that an unknown source is not treated with the same credibility and thus not acted upon by responders. This is similarly argued by Gürses and Preneel (2016), who acknowledge that claims about anonymising data providing sufficient protection to data subjects are misleading because of the assumption that anonymity is a form of personal security. This can be an added challenge when quality assurance and validation come predominately from socialisation practices.

Finally, the processing performed by aqua3S should as far as possible be isolated from general legacy/agency systems, which are highly likely to contain sensitive personal data which should not be used within the aqua3S.

7.1.2 Documentation

Controllers need to implement a range of measures to ensure compliance with their obligations under the GDPR. This includes implementing measures to objectively demonstrate such compliance. This means that controllers will need to document their data protection efforts and, if requested, make such documentation available to authorities. Any data protection measures implemented will also need to be periodically reviewed and updated as appropriate.

Controllers (Article 30(1) of the GDPR) and processors (Article 30(2) of the GDPR) both have documentation obligations. Documents must include processing purposes, data sharing and retention, and be kept in writing. The documentation must also be granular enough to be meaningful and include links between different pieces of information. This can also help improve data governance. Documentation needs to include:[7]

- The name and contact details of the consortium and organisation (and where applicable, of other controllers, your representative and your data protection officer).
- The purposes of the processing.
- A description of the categories of individuals and categories of personal data.
- The categories of recipients of personal data.
- Details of transfers to third countries including documenting the transfer mechanism safeguards in place.
- Retention schedules.
- A description of technical and organisational security measures.

[7] For more details about this list, see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/

7.1.3 Transparency with regards to privacy-related activities

Responsible data processing implies that there is awareness (paired with choice and consent or contract) on the part of the data subject with regard to the processing of their data. Under the GDPR, personal data can only be processed if the data subject has unambiguously given consent or signed a contract. Consent must be meaningful: given freely after the person has informed of nature, significance, implications and risks. aqua3S' exercises and demonstration activities should therefore be fundamentally based upon user consent for all processing of personal data. Furthermore, aqua3S should be designed in a way that a contractual basis for processing can be established. This is important because once the system or components are taken up within an organisation, the employees cannot give meaningful consent, because they are under contract and in many cases will not be able to freely refuse. These will need to be represented in the software functionality.

A fundamental concern is to ensure that data subjects are actually aware of the data processing practices being used in aqua3S (as deployed in a specific context). This helps to meet legislative requirements around informed consent and accountability.[8] Even more, supporting end users in understanding how the platform is data processing contributes to usability and helps build trust in the system and fellow users.

This means that:

- the data subject should be informed of the data controller's data processing practices before any personal information is collected
- the default settings should be privacy protecting
- the data subject is aware of the implications of sharing their data, the details of how the data will be used and shared, and that they are then able to control how this data is shared

The most common approach to this issue is privacy notices and polices. These include:

- what (kinds of) data are processed (collected, used, shared and stored)
- the purpose and the legal base for data processing
- how and by whom data can be accessed
- data retention period or, if this is not established, the criteria used to determine that period
- the (data protection) rights awarded data subjects
- the protocol for deletion of data
- identification of data controller
- data protection officer (DPO) contact details

While privacy notices or terms of use may set out the basis for data processing practices, such texts are not always understandable or effective. Most commonly, privacy notices and terms of use are simply accepted by users without any engagement. However, the GDPR requires affirmative, informed, and active (opt-in) consent prior to the start of any processing operations. aqua3S should therefore pursue alternative ways of presenting privacy related information and ensure they are

[8] e.g. GDPR Article 12- Transparency and facilitation in the exercise of the rights of the data subjects; Article 13- Right to information; Article 15- Right to access data; Article 16- Right to rectification; Article 17- Right to erasure 'right to be forgotten'

written in clear and simple language that end-users will actually read and understand (Bogdanovic et al 2009, Coles-Kemp & Kani-Zabihi 2010). aqua3S might explore:

- consider how best to provide useful information to the various users, and at what points in the user experience this should be done to best assist them in understanding the information they are sharing
- context-relevant notifications, including during system usage
- develop prompts, labelling and signposting at appropriate points in the user experience/interface to ensure an awareness of these differentials
- visualisations of which other users have access to what personal or sensitive data

In order to ensure that users are aware, the project will itself need a clear picture of the personal and sensitive categories data that is being collected, and how this data is being used.

7.1.4 User control

aqua3S should limit the amount personal information is visible to other users of the system. Design should start from the presumption that none of this needs to be visible. If visibility becomes a necessity, it needs to be justified based upon clear and unambiguous purpose. The system could automatically modulate resolution and granularity of personal data to different purposes to support appropriate, yet limited, visibility. Allowing for multi-layered privacy settings that give the user complete control over what information is visible, and to whom, could be a way of addressing this concern. This could mean, for instance, that users can determine what information – and at what granularity - about their location, decisions, informational searches and communications during training is stored and accessible by other users.

7.1.5 User Consent and Contract

Usage of personal data requires consent from the data subject or explicit statements within data subjects contract. A data subject has to give his/her consent or sign a contract before any information is collected. Any change in the conditions of the data processing demands the renewal of consent or contract. It is important to ensure that informed consent is meaningful or that contract language is clear and precise in that users are aware of the privacy implications of engaging with the system. Different processing activities or purposes should be consented separately.

7.1.6 Human-Readable Transparency

Perspectives from Human-computer-interaction (HCI), which is the study of interfaces between people and computers, suggest that good design of the underlying system, and the interface to that system, is essential; poorly designed system and interface that creates errors or undesirable outcomes during use, including loss of information or privacy, is something that should be avoided. (Wills & Reeves 2009). Moreover, a complicated interface can exclude those with less technological experience, systemically – if unintentionally – discriminating based on technological capabilities. This can be partially achieved by being transparent, both linguistically and conceptually, so users can understand, though use, the implications of how they are using aqua3S. They also need transparent explanations of how aqua3S is processing data (non-personal included) to determine if the results are relevant to their actions or how the more generic rules that define the system relate to their specific situation and standards of practice. Because data cleaning activities can support privacy (e.g. differential privacy) or – on the contrary - create situations of data bias, these activities should be included in such

documentation. End-users should also be allowed to monitor processing and automated algorithms to understand what data was used and how it was used to arrive at a conclusion. Producing these documents during design can help end-users and designers know when they need to support privacy or non-discrimination activities, or when organisational actions will suffice. This will also help users do their own risk mitigation practices when engaging with data aggregation, and not leave all risk measure to the technology itself.

7.1.7 Clear Rights and Responsibilities of End-Users

Because information sharing can be limited, the question arises as to who has the right to access the data and when do they have those rights (for example, does an actor's access rights change between planning and response). All actors who could process data of any kind should be identified. There should be clear divisions of roles and responsibilities determined prior to use. These roles should have technological counterparts (e.g. related to role-based access) so that use rights match use capabilities and avoid accidental misuse of data. This can also be reversed, where all technological stages have human counterpart. For example, any given insight or suggestion provided by the system could require human approval for continuation.

7.1.8 Security and access control

aqua3S should not be blind plug-in for users; they should have some access to what is going on within the data processing. This is in part because organisations are legally required under the GDPR (Article 32) to implement appropriate technical and organisational measures designed to ensure level of security appropriate for risk. This includes designing with secure coding standards and practices, clear understandings of when encryption can be used without increasing accessibility issues, and backup systems. But this also should include data access and management policies, personnel training, and internal audit protocols.

The consortium should check system security in multiple different data sharing contexts with organisations covering range of security practices.

7.1.9 Role-based access control

Already part of the user requirements, role-base access could be employed in different ways. The system could be designed so that only trainees can see their profiles and traces of the activities; such a system provides the strongest privacy and ethical protections. However, this impedes organisational learning and collaborative planning, where sharing exercise results with other responders can enhance interoperability. This access should be secured based upon consent/contract, role, and purpose. For example, to gain access to a trainee's record, a planner should have consent of the trainee and also formal management responsibility for that trainee's growth and development. A registry of accesses (e.g. a recoverable log of the actions that take place through the aqua3S platform) would help to avoid unexpected or inappropriate stakeholders from illegitimately accessing person information.

7.1.10 Actively Engage Diversity

Because how we engage with technology helps us learn more about events or issues, influencing how we think, not just augmenting how we already thought beforehand (Hutchins 1995), it is possible to turn the risk of bias on its head; for example, this could be achieved Including results that do not fit expectations in order to help users think outside of their boxes in ways that make collaboration more

possible. A focus on diversity could help address bias that might be built into a system and encourage parallel shifts in organisational culture.

This could be addressed by allowing end-users to insert new rules into the system to address diversity needs they identify, from different decision-making structures to different demographical categorisations. How the system is currently defining terms, actors, and features should be conveyed to the user at an appropriate point in the user experience, and it should not require end-users to discover differences from their local usages on their own.

7.1.11 Provide Interpretive Context and support for Determining Data Quality

Background information, termed interpretive context, helps users understand the how and why of a given piece of data. It can help users notice, determine, and improve the relevance, quality, timeliness, appropriateness, and compatibility of the data provided in the system (Bertelsen and Bødker 2001). However, such activities need to not be cumbersome, burdensome, and cost-ineffective. Having such context can also help inform end-users regarding data quality: depending on the incident, the resolution of an image or data collected could be adjusted and end users need thus contextual data to understand how best to do that.

This context could also help make more visible sensitive data or vulnerable groups to end-users. For example, explaining how categories were arrived at could help end-users see that a local population would go unrepresented. Providing in advance all the data that a drone could capture as a list in the handbook could help end-users select data resolution to avoid incidental sensitive data gathering.

7.1.12 Security

As technological innovation is frequently built into existing legacy systems, it is necessary to ensure that retrofitting innovation does not ignore the concern that legacy systems may include because they are outdated and therefore vulnerable to infiltration. As outlined in section 5.4.2.1. 'societal vulnerability' where unpatched code remains, innovation measures must seek to actively address and overcome these challenges (Adepu et al. 2019).

In order to chart the levels and nature of cyber-vulnerability, a focus on the underlying structural issues that may lead to such vulnerability is the key. Here, a drive to reduce costs appears to be a motivator to enhance remote sensing and control capabilities of water infrastructures. Does this drive results from a profit focus to drive down costs at the expense of the community and result from an underfunding of the water sector? Understanding why such tools are in place can point to what kinds of mitigation measures are needed to reduce these new risks. Some could continue to be technical, like regular system or sensor updates. Some are political or organisational, including staff training to avoid human error, new regulations to manage silent polluters, or increased government funding (Germano 2018). Some require resources for the immediate moment, and others require resources throughout a longer water or pollutant lifecycle. Sufficient attention needs to be paid to the continuing costs necessary to upkeep the cyber security framework. The development of such systems is not a one-off event, and the failure to update both the technology, both the socio-economic and political systems that support them may mean that they do not keep pace with the advancement and innovation of malicious threats, reopening water networks to potential harm (Adepu et al. 2019).

Additionally, users of the aqua3S system should be attuned to the need to continually safeguard systems from cyber-threats. Regular training (across various levels of seniority (Germano 2018) as well

as system maintenance will be necessary. As such, it is important to identify where there will be a consistent stream of resources that will be able to be dedicated to the aqua3S system.

Recognising that cyber-security will remain an ever-present threat, efforts should be made to restrict information that could allow for water networks to be compromised. As such, considerations like the information of individual sensors in the water network to be obscured – and displayed at aggregate level to users who do not need to know the specific locations.

7.1.13 Compliance with drone regulations

The recommendations highlighted in section 5.4.1.2. UAVs (Drones) should be followed throughout the project, as well as in the future use of the developed system.

7.1.14 Decision-making

The use of the aqua3S system will ultimately affect how users interact with the water network. As such, the presentation of additional information may ultimately have an impact on how users assess and weigh information necessary for responses to anomalies in the water system. During the course of the project and deployment, attention should be paid to how users interact with this system and how the system itself affects and influences decision-making process as a whole.

Ultimately, the aqua3S system will provide information on selected issues. As such, additional information will be required in order to determine ideal responses (for instance, in relation to human vulnerability). The boundaries and limits of the aqua3S system should be acknowledged and appreciated, and specific efforts taken to gather the additional information that is necessary for ethical decision making.

7.2 Framework informed non-functional requirements

7.2.1 Human and environment-centric analysis and response

Measures taken to address water security should place humans and the environment at the centre of these responses. This is designed to place the right to water at the centre of activities and that this will ultimately dictate response measures and prioritisation. These approaches, however, should attempt to avoid paternalist tendencies; rather, they should seek to empower communities and facilitate their ability to exercise their agency.

This will be diffused through the aqua3S project in a number of ways. For example, the emphasis on consent in the data collection seeks to appreciate the individual as a rights-holder and recognises their dignity and agency. However, the respect for individual and community dignity and agency should also be upheld in other domains; for instance, in terms of providing information on the project and demonstrations within the community, in attempts to engage the community to identify how to best interact with and respond to their needs in a participatory manner. This is should reflect the right to *seek, receive and impart information* concerning water issues.

7.2.2 Societal Trust

The need to foster societal trust in the system is essential for the long-term viability of the solution, as well as to ensure the aqua3S solution is accepted by communities. This depends on two important considerations:

- that the aqua3S system provides societal benefits
- that the communities it concerns understand the system and have recourse where the system infringes on their rights.

While the former pertains to the points mentioned above, the latter point can be brought about by active efforts to communicate the nature of the system, its purpose and objectives, the tools used, as well as the ways in which it attempts to limit impacts. This can be achieved through by notifying the public about the deployment of the project, prior to any such efforts, in an accessible language (in terms of language and content). The notification efforts should utilise a range of publicly available mediums, such as social media, the press and other similar notification processes with indications on where to seek further information. Further, contact points should be highlighted so that the local community can relay any concerns and specifically request information or actions in relation to any captured personal data.

7.2.3 Incorporating an intersectional lens to vulnerability analysis and response measures

In order to fully realise how communities are impacted, further disaggregation is necessary. Certainly, characteristics such as class, legal status, urbanization amongst others impact how we interact with water, and will inform our response measures.

For instance, where individuals have access to self-contained water tanks or have the ability to purchase bottled water, their resilience will be different to those who cannot afford such mitigation measures. Additionally, individuals without formal resident status will necessarily feel less able to raise concerns to water boards. Here, we should recognize that a 'one size fits all' approach will leave vulnerable groups outside of our protection. As such, attempts to improve water resilience must incorporate the voices of diverse communities and build respect for marginalized communities at its core.

In doing so, an intersectional approach to water security can add positive value to efforts designed to prevent and mitigate water insecurity. By developing an accurate understanding of vulnerability, it is possible to ascertain where resultant harms will be the most severe and tailor our responses accordingly, prioritizing those most affected, or ensuring that the response measures are suited to specific communities' needs.

Such approaches should ultimately recognise the specific contexts of the relevant communities to appreciate their resilience, vulnerability and their specific requirements for responses. As such the linguistic requirements and access to communication channels will be essential considerations.

7.2.4 Societal Benefits

The aqua3S project has the potential to considerably improve efficiency within the water sector. Should the societal benefits be actualised, the benefits should go towards the community as a whole. The reduction in costs needed for the system should be therefore be used for the decrease in costs and/or the redirection of resources to other areas for the public good as opposed to solely increasing income for the executive staff and shareholders.

Moreover, with regard to the future use of the aqua3S solution beyond the scope of the immediate project, where the increased efficiency results in a need for fewer staff members, consultations should be held with workers, and indeed with relevant trade unions representing such workers, in order to minimise the impacts and/or need for a reduction in employment.

8. Conclusion and next steps

This report describes and analyses the initial results from the E/PIA process for aqua3S in order to provide a preliminary ethics and legal framework; the document includes the ethical, legal, societal, and privacy issues that arise as a result of the technologies that will be implemented in aqua3S and design decisions being made within the project. These issues are derived from a general analysis of the high-level project concept, interviews with technology partners to understand the flow of data throughout the aqua3S platform, discussions between end-users and technology partners at the E/PIA workshop, considerations of the user requirements, and legal and background analysis. Issues that need to be addressed during the aqua3S project design are highlighted. However, risks and issues that will arise beyond the end of the aqua3S project are also included, because their considerations could improve not only changes for uptake and sustainability, but also enhance aqua3S as a tool for public good. A final listing of key issues was provided in section 7 to help provide overarching guidance for aqua3S consortium members.

In order to support technical-partners in addressing these challenges, high-level solutions are proposed. It is expected that these solutions are preliminary starting points for further exploration, not the actual solutions to be implemented. Further work during the design process with technology partners and end-users will be needed in order to being to articulate implementable solutions.

The next ethics and legal framework deliverable, D2.5 (due in month 32) will include reporting upon on-going work alongside WP2. It will also incorporate additional inputs from the end user front to ground the recommendations in practice and technology in use.

This will include engaging with end-users and technology partners during and after pilots, in order to take these high-level issues and recommendations and translate them into more specific functionalities and specifications for aqua3S.

It will also include work on finding the best ways to make users of the aqua3S aware of the potential privacy implications of use of the systemand supporting them in making informed choices and active, informed consent. This will support any work necessary for the upcoming training manual in Task 8.3 (User Training) to make privacy and ethical guidance understandable and meaningful to users.

8.1 Honing recommendations

The development of the ethics and legal framework is not a static event. The iterative development of the framework from D2.2 to D2.5 implies that as the awareness of ethics and legal issues is going to be raised, the framework will be amended to reflect the evolution and fine-tuning of our understanding. Moreover, as project partners engage with the initial framework put forward within this deliverable, more insights may be gathered from subsequent ethics and legal discussions within the consortium, with may in turn feed into future ethics and legal tasks.

This pertains the development of the aqua3S solution and the way it operates, the contexts of the pilots, as well as any developments in legislation, case law and regulatory governance (national and international) that may come to affect the aqua3S project and our understanding of the ethics and legal considerations. Where these developments occur, the ethics and legal framework will be iteratively calibrated to reflect this.

Ultimately, the more high-level nature of this deliverable will be calibrated to become increasingly specific. As a result, the final ethics and legal framework will not only contain discussion and guidance

on thematic ethics and legal issues, but also specific recommendations on how the issues should be addressed and how the system should be deployed in future.

8.2 Standardisation

The aqua3S project seeks to develop guidance for the development and implementation of future of water security standards (see WP9). Task 9.3 ('Guidance for responsible applications of water security standards and policy') of WP9 'Policies, Information Management & Standardisation' seeks to conduct a pre-standardisation impact assessment and develop guidance to responsible (e.g. ethical, societally conscious) impact from and applications of any proposed standards or policy to assess their impact is inclusive and offers whole-society resilience (without leaving any groups unintentionally behind). The related deliverable (D9.3 'Guidance for responsible applications of water security standards and policy') will provide a pre-standardisation framework that will expand on the ethics and legal risks and opportunities that have been identified and explored within this deliverable. It will also look incorporate additional ethics and legal risks and opportunities where identified though future research and developments within the aqua3S project. Within D9.3, the identified ethics and legal issues will be outlined in direct and precise language and will be raised to those seeking to apply standards. As such, the ethics and legal risks and challenges will be specifically highlighted and imbedded in the pre-standardisation and standardisation process, as a required consideration for applying standards. This will take inspiration and build on the standardisation assessment framework model developed in the H2020 ResiStand project (Grant agreement 700389).

8.3 Conclusion

This deliverable outlines a number of the ethics and legal issues that are active within the aqua3S project. This, however, is by no means an exhaustive list of the relevant issues, and additional considerations will be reviewed, researched and addressed where relevant. Certainly, the values of the project and legal obligations are articulated throughout this document in a manner that can help to direct the project towards in an ethical, legally compliant and responsible manner throughout the project.

However, as highlighted above, it must be borne in mind that, at the current project development stage, a number of these issues remain nascent. Where possible these issues must be resolved, however, in a number of situations, the issues require monitoring and the collection of information (for example, from users during pilots). As our understanding of the project (both in terms of its development and deployment), these issues will be further articulated, researched and specified throughout the lifecycle of the project. Ethics and legal monitoring will continue to be conducted at the research and development stage and will be complemented by ethics and legal monitoring during the pilot testing. It will therefore provide a more real-world lens to how the aqua3S project will operate in a functional setting. Furthermore, the engagement of research participants within the pilots will require a proper monitoring to ensure that the rights of participants will not be negatively affected through the course of the project.

This deliverable has highlighted a number of issues to be considered by the consortium as a whole, providing an ethics and legal backdrop to inform and guide the project on a range of matters, from privacy and GDPR compliance, as well as non-discrimination, enhancing participation and other legislative compliance (e.g. with regard to UAVs).

9. References

Adepu, S., et al., Investigation of Cyber Attacks on a Water Distribution System, ArXiv abs/1906.02279, 2019.

Alston, P. (2018) Privatization and human rights, Oral statement at the UN General Assembly, A/73/396. Accessed: https://srpovertyorg.files.wordpress.com/2018/10/a_73_396-sr-on-extreme-poverty-privatization.pdf

Ashton, K. (2019) Darwin's Lord Mayor dismisses privacy fears of 'smart city conspiracy theorists, ABC News, accessed: https://www.abc.net.au/news/2019-06-13/darwin-smart-city-rollout-privacy-concerns-dismissed-lord-mayor/11203528

Baudoin, M.-A., Henly-Shepard, S., Fernando, N., Sitati, A., & Zommers, Z. (2016). From Top-Down to "Community-Centric" Approaches to Early Warning Systems: Exploring Pathways to Improve Disaster Risk Reduction Through Community Participation. International Journal of Disaster Risk Science, 7(2), 163–174.

Becker, M 2019, 'Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy', Ethics and Information Technology 21, pp. 307–317.

Bertelsen, O. W., & Bødker, S. (2001). Cooperation in massively distributed information spaces. In ECSCW01 Proceedings of the seventh conference on European Conference on Computer Supported Cooperative Work. Kluwer Academic Publishers. pp. 1–17. Retrieved from http://portal.acm.org/citation.cfm?id=1241868

Bloustein, E 1964, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser",New York University Law Review, 39: 962–1007

Bogdanovic, D., Crawford, C. & Coles-Kemp, L. (2009). The need for enhanced privacy and consent dialogues. Information Security Technical Report. 14(3). 167-172

Brey, P. (2000) Disclosive Computer Ethics. Computers and Society, 30(4), pp. 10–16.

Brown et al., (2019) Gender Transformative Early Warning Systems: Experiences from Nepal and Peru, Rugby, UK: Practical Action

Campo, S. R., Howarth, C. N., Raymond, N. A. & Scarnecchia, D.P. (2018). The Signal Code: Ethical Obligations for Humanitarian Information Activities. Signal Program on Human Security and Technology, Standards and Ethics Series: 03. Cambridge: Harvard Humanitarian Initiative.

Carroll, J. M. (2000). Five reasons for scenario-based design. Interacting with Computers, 13, pp. 43–60.

Christiansen, F., Rojano-Doñate, L., Madsen, P. T., & Bejder, L. (2016). Noise levels of multi-rotor unmanned aerial vehicles with implications for potential underwater impacts on marine mammals. Frontiers in Marine Science, 3, 277.

Cohen, J 2002,Regulating Intimacy: A New Legal Paradigm, Princeton: Princeton University Press

Deeks, A., Lubell, N., & Murray, D. (2019). Machine learning, artificial intelligence, and the use of force by states. J. Nat'l Sec. L. & Pol'y, 10, 1.

Deloite, C. (2017). Global mobile consumer trends.

Directorate-General for Communication Special Eurobarometer 431 Report on Data Protection 2015, Survey Conducted by TNSOpinion & Social: https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf

Esposito, F., Westchester village finds clever solution to thwart hacking of critical infrastructure, Rockland/Westchester Journal News, 8 January 2020. [Online]. Available: Available at: https://eu.lohud.com/story/news/local/westchester/rye-brook/2020/01/08/iran-hacked-rye-brook-dam-2013/2846127001/ [Accessed 17 April 2020].

European Political Strategy Centre. (2018). Report from the High-Level Hearing 'A European Union Strategy for Artificial Intelligence'. https://ec.europa.eu/epsc/sites/epsc/files/epsc_-_report_-_hearing_-_a_european_union_strategy_for_artificial_intelligence.pdf

Finn, R, D Wright, and M Freidewald 2013, European Data Protection: Coming of Age. S. Gutwirth et al. (eds.). Dordrecht: Springer.

Floridi, L. (1999). Information ethics: On the philosophical foundation of computer ethics. Ethics and Information Technology, 1(1), pp. 33–52.

Fried, C 1970,An Anatomy of Values, Cambridge: Harvard University Press.

Gerety, T 1977, 'Redefining Privacy', Harvard Civil Rights-Civil Liberties Law Review, 12: 233-96.

Germano, J. H., Cybersecurity Risk and Responsibility in the Water Sector, American Water Works Association, 2018.

Gerstein, R 1978, 'Intimacy and Privacy', Ethics, 89: 76–81.

Gürses, S. & Preneel, B. (2016). "Cryptology and Privacy in the context of Big Data", in van der Sloot, B., Broeders, D. & Schrijvers, E. (Eds), Exploring the boundaries of big data. WWR The Netherlands Scientific Council for Government Policy. Amsterdam: Amsterdam University Press.

Kroener, Inga, and David Wright, "Privacy Impact Assessment Policy Issues" in Artemi Rallo Lombarte and Rosario Garcia Mahamut (eds.) Hacia Un Nuevo Derecho Europeo De Protección De Datos. Towards A New European Data Protection Regime, Tirant lo Blanch, Valencia, 2015

Keats Citron, D. (2008) Technological Due Process, 85 Wash. U. L. Rev. 1249, 1252.

Kloza, D., Van Dijk, N., Gellert, R., Böröcz, I., Tanas, A., Mantovani, E. & Quinn, P. (2017). Data Protection Impact Assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals. d.pia.lab Policy Brief No. 1/2017.

Kupfer, J 1987, "Privacy, Autonomy and Self-Concept",American Philosophical Quarterly, 24: 81–89

Marchezini, V., Trajber, R., Olivato, D., Munoz, V. A., de Oliveira Pereira, F., & Luz, A. E. O. (2017). Participatory early warning systems: youth, citizen science, and intergenerational dialogues on disaster risk reduction in Brazil. International Journal of Disaster Risk Science, 8(4), 390-401.

Maurer, S. M., Firestone, R. B., & Scriver, C. R. (2000). Science's neglected legacy. Nature, 405(6783), pp. 117–120. http://dx.doi.org/10.1038/35012169

Mellon, J., & Prosser, C. 2017). Twitter and Facebook are not Representative of the General Population: Political Attitudes and Demographics of British Social Media users. Research & Politics.

Mordini, E., Wright, D., Wadhwa, K., De Hert, P., Mantovani, E., Thestrup, J., Van Steendam, G., D'Amico, A. & Vater, I., (2009) "Senior citizens and the ethics of e-inclusion". Ethics and Information Technology, Vol. 11 Issue 3, pp. 203–220

Narayanan, A. & Shmatikov, V. (2010). Myths and Fallacies of Personally Identifiable Information. Communications of the ACM 53(6), pp. 24-26.

Nelson, L. (2011). 'Anonymity', in America identified: Biometric technology and society. Cambridge, MA: The MIT Press.

Nissenbaum, H. (1998). Values in the design of computer systems. Computers in Society, 28(1), pp. 38–39.

Nissenbaum, H 2009, Privacy in context: Technology, policy and the integrity of social life, Stanford, Stanford University Press

Penissat, E., Spire, A., & Hugrée, C. (2020). Social Class in Europe: New Inequalities in the Old World. Verso.

Perrow, C. (1984). Normal Accidents: Living with High-Risk Technologies. Princeton, NJ: Princeton University Press.

Petersen, K., Buscher, M., & Easton, C. (2017). On anonymity in disasters: Socio-technical practices in emergency management. Ephemera: Theory and Politics in Organization, 17(2), pp. 307-326.

Qawasmeh, E., Tawalbeh, M., & Abdullah, M. (2019). Automatic Identification of Fake News Using Deep Learning. 2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS).

Regan, P 1995,Legislating Privacy, Chapel Hill, NC: University of North Carolina Press.

Sajid, A., Abbas, H. & Saleem, K., Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges, IEEE Access, vol. 4, p. 1375–1384, 2016

Solove, D 2008,Understanding Privacy, Cambridge, MA: Harvard University Press.

Udu-gama, N. (2009). Mobile cell broadcasting for commercial use and public warning in the Maldives. Sri Lanka: LIRNEasia. Accessed: http://preparecenter.org/sites/default/files/11235_cbmaldivesfinal20090 411.pdf

Webster, C. W. R., & Leleux, C. (2019). Searching for the real sustainable smart city? Information Polity, 1–16. doi:10.3233/ip-190132

Wright, D. (2012). The state of the art in privacy impact assessment. Computer Law & Security Review, 28, pp. 54–61.

Vaughan, D. (1996). The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA. Chicago: University of Chicago Press.

Verbeek, P.-P. (2011). Moralizing Technology: Understanding and Designing the Morality of Things. Chicago, University of Chicago Press.

Wright, D. & Friedewald, M. (2013). Integrating privacy and ethical impact assessments. Science and Public Policy, 40(6), pp. 755-766.

ANNEX A – Risks and opportunities identified in the ethics workshop

As referenced in section 4.2.2, two half day ethics workshops were held on 3th and 4th of June 2020 respectively. These workshops were held online due to the ongoing coronavirus pandemic, and utilised a range of tools including Microsoft Teams, Mentimeter and Mural.co services. During this workshop, participants were asked to collaboratively identify and discuss the ethics risks and opportunities that are relevant to the aqua3S. The following images demonstrate the ethics workshop agenda, as well as the interactive boards developed by participants.

Figure 4. Ethics workshop agenda - 4th June 2020

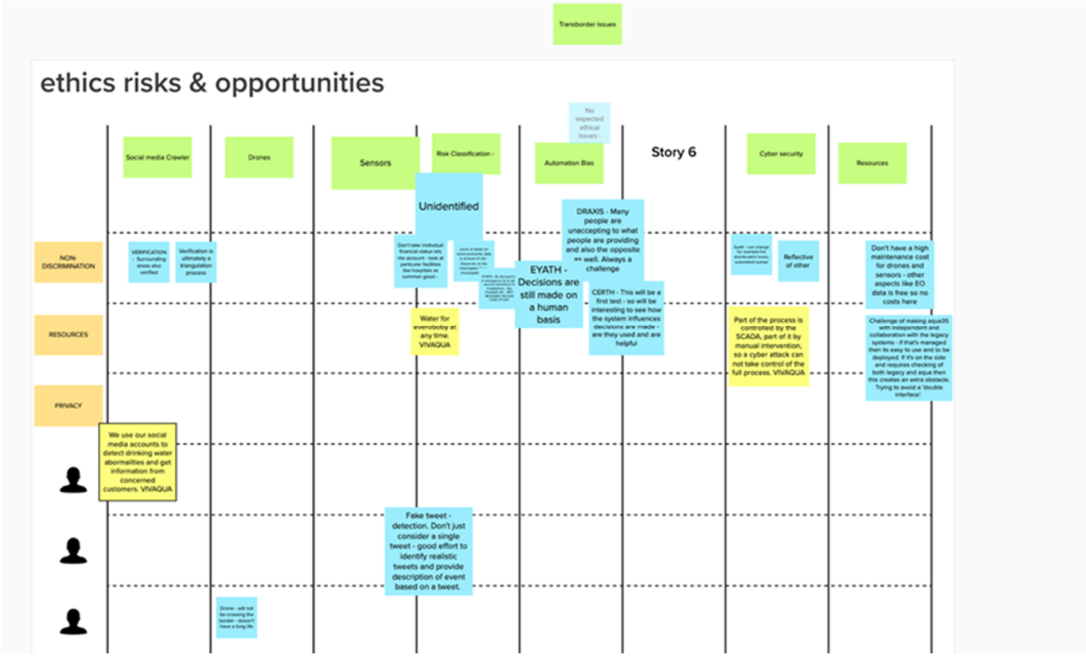

Figure 5. Ethics workshop collaborative notes on ethical risks and opportunities – 3rd June 2020

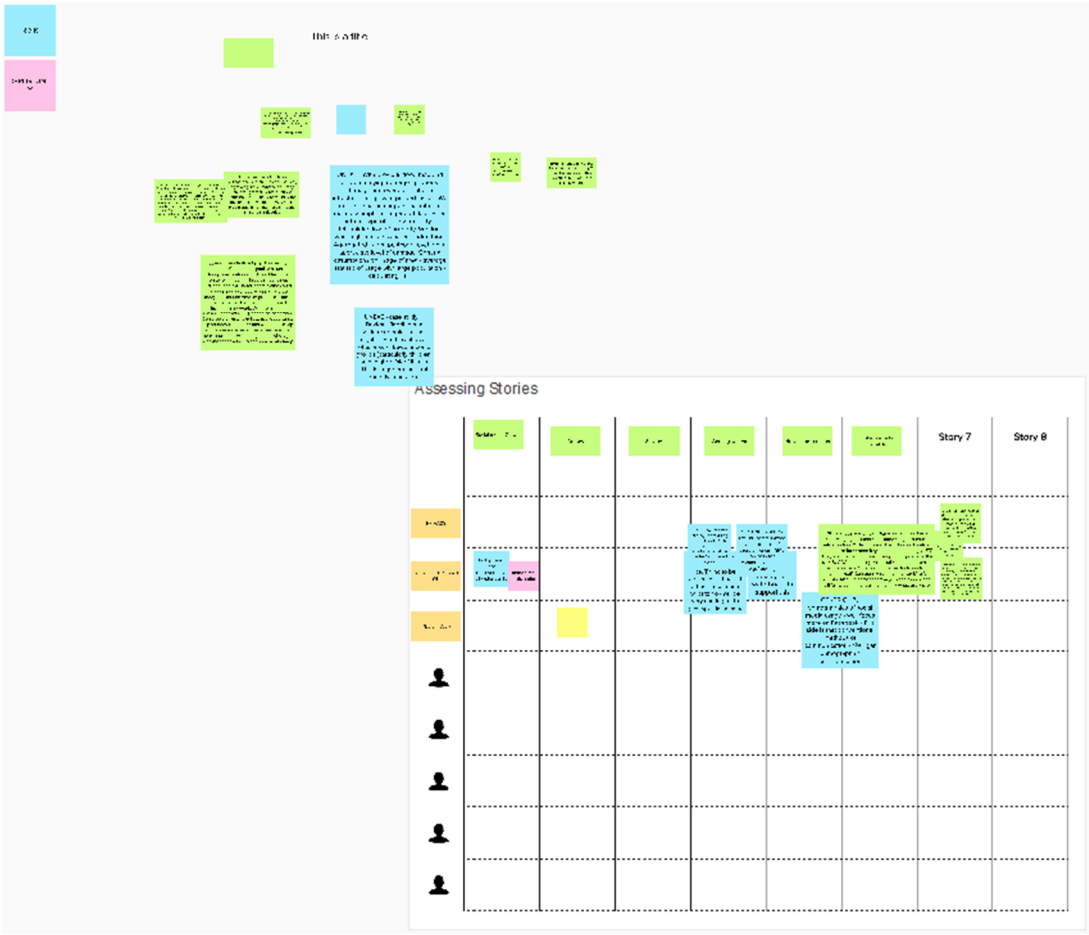

Figure 6. Ethics workshop collaborative notes on ethical risks and opportunities – 4th June 2020

ANNEX B – aqua3S Anonymity Protocol

This annex contains the Anonymity Protocol that has been provided to the consortium members and adhered to within aqua3S.

aqua3S Anonymity Protocol

Taking guidance from the EU Opinion 05/2014 on Anonymisation Techniques, as well as the UK Information Commission Office's Anonymisation: managing data protection risk code of practice (2012) and the UK Data Archive's advice on anonymisation of qualitative data (see: http://www.data-archive.ac.uk), this Anonymisation Guide aims to help aqua3S members protect the rights and privacy of research participants.

Please note that there is no one-size-fits-all fool-proof process of anonymization and reflect critically upon case-by-case concerns regarding anonymization.

During data collection

- Avoid collecting unnecessary personal data. For example, it is not necessary to record people's full names or their home or work addresses. The less personal data collected, the less depersonalization work to do.
- During data collection make mental notes of any potentially sensitive information that arises. For example, someone might disclose a medical condition during an interview and such information has to be treated with the upmost confidentiality (see 'risk assessment' below).

After data collection: Storing personal data

- All personal data should be immediately transferred to encrypted, secure and password protected servers or devices. If you use a mobile device to record data, make sure it is encrypted and transfer data to secure servers or devices as soon as possible.

After data collection: Processing personal data into depersonalized data

- Before data can be used, it must be depersonalized, unless we have an agreement with the research participant that says otherwise, e.g. in the case of photos. However, even in the latter case, we must consider how the identification of one research participant who has given consent to be identified could impact on the possibilities of identifying another research participant who has not given consent to be identified.
    - Pseudonymisation refers to the process of replacing a personal identifier (e.g. name) or semi-obvious identifier (e.g. postal code) with a pseudonym, tag, or coded reference. In this case, the data is altered in that it cannot be related to the particular research participant in which it came from. In order for this to be successful, all potential identifiers need to be changed and/or replaced. This is especially important for aqua3S when dealing with case studies. For example, even if we use a pseudonym for an official involved in disaster response, if we refer directly to the specific incident it would be possible to infer who was the official. In such cases, it would be advisable to use a coded reference for the event, e.g. instead of 'contamination of Kouris dam' we could refer to the contamination of 'a large dam.' This last example could also be considered a form of abstraction.
    - Abstraction and generalization refer to the process of de-contextualizing data to allow for greater anonymity, while simultaneously retaining enough contextual information

to be useful. For example, rather than provide exact geographical locations (e.g. the name of a village or city), more general geographical locations can be used, such as regions (i.e. the west coast of Ireland) or even countries (i.e. the Republic of Ireland).

- The UK Data Archive (http://www.data-archive.ac.uk) further suggests that researchers:
  - use pseudonyms or replacements that are consistent within the research team and throughout the project, e.g. use the same pseudonyms in publications or follow-up research
  - use 'search and replace' techniques carefully so that unintended changes are not made, and misspelled words are not missed
  - identify replacements in text clearly, e.g. with [brackets] or using XML tags such as word to be anonymised
  - create an anonymisation log of all replacements, aggregations or removals made - store such a log separately from the anonymised data files.

- aqua3S will store copies of some personal data securely. In order to make sure that you maintain the ability to link personal data with depersonalized data (e.g. for the purpose of providing participants with a sense of where their pseudonomised contributions enter into reports or publications), each data piece should be given a unique identification number (e.g. 000001), which will be recorded in a 'key'. The 'key' should be kept in secure and encrypted form separately from both the personal and depersonalized data.
- If data is given with the expectation of confidentiality, the original personal data should be deleted as soon as possible and this status should be clearly marked (e.g. 000001-C).
  - Depersonalizing textual data (e.g. transcriptions of recorded interviews; unpublished documents)
    - Remove all obvious identifiers or semi-obvious identifiers which could be used to identify any individual research participant (unless we have an agreement with the research participant that says otherwise). The aqua3S team will engage in both pseudonymisation and abstraction in order to give the highest level of anonymisation possible within the boundaries of working with qualitative data in the project.
  - Depersonalizing audio/visual data (e.g. voice recordings, photos)
    - aqua3S research participants will be asked for their consent to be recorded, photographed, and/or filmed; they will also be asked if they consent to our use of these materials in publications for a wider audience.
    - A person's voice is recognisable and therefore personal data. Audio recordings can be depersonalized by transcribing them and by using pseudonymisation and abstraction techniques.
    - In some cases, research participants will consent to aqua3S' use of their voice recordings or photos in publications. aqu3S team members are responsible for informing other team members of any cases in which this consent is not given (e.g. by marking the data with 000001- NV). In the event that such consent is not given, depersonalization of audio recordings or photos will be done using computer software. This will include the altering of voice, the blurring of faces, and the bleeping out of names or locations

See examples in the table below for how we propose to use data replacements.

Original	Replace with:
Vivaqua employee	Water company employee
Alexandra (real name)	Sofia (pseudonym)
St Vincent's University Hospital	A hospital in Dublin

Table 2. Data Replacement exmaples

After data collection: Sharing personal and depersonalized data between aqua3S members

- Personal data can only be shared among aqua3S members who have gained authorization from their relevant authorities and who have signed the Research Ethics Code of Conduct. Even when this is the case, the transfer of personal data between aqua3S members has to be done in the most secure fashion and in compliance with the Research Ethics Protocols. It can be done face-to-face and through encrypted digital communications and file transfers.
- Depersonalized data can be shared between aqua3S members, even if they do not have authorization. The transfer of data between aqua3S members has to be done in the most secure fashion and in compliance with the protocols in the Research Ethics Protocols. It can be done face-to-face and through encrypted digital communications and file transfers.

After data collection: Risk assessment of re-identification

- Re-identification risk assessment, the likelihood that an individual research participant could be identified from pieces of depersonalised data, is an ongoing process. There are several strategies you can use for this:
- The EU Opinion 05/2014 on Anonymisation Techniques refers to assessing risk based on 'all the means likely reasonable to be used' (p. 3). Data producers are asked to assess the likelihood (i.e. is there value in reidentification) and the ability of other persons (i.e. reasonable means with regards to time, cost and skill) to re-identify data subjects.
- The UK Information Commissioner's Office suggests adopting 'a 'motivated intruder' test as part of a risk assessment.' (2012: 23). This includes exchanging excerpts of depersonalized data within the consortium in order to assess whether the depersonalization of qualitative data has been successful.
- Assess potential for harm. Risk assessment should ask what the harm to research participants would be if there was to be re-identification, especially with a view to data deemed sensitive. aqua3S suggests two approaches to this. First, any data that could bring harm to research participants if re-identification were to take place should be considered sensitive. Second, research participants should be asked to help to decide whether data should be deemed sensitive or not. This includes asking research participants to clarify on consent forms whether the information that they provide is given with the expectation of confidentiality. Data deemed sensitive will face greater scrutiny in regards to how or if it should be used and/or shared outside the aqua3S consortium. Sensitive personal data will be deleted as soon as possible.

Drones and data minimization

Drone operators and pilots will deploy drones and conduct flights in a manner that minimizes the collection of personal data, as per the data minimization principle. Where data subjects have provided

their consent to being recorded by drones, the drone pilots and operators should only collect data that has been consented to by the data subject.

To achieve this minimization of the capture of personal data or the interference with privacy, drone pilots should capture unconsenting and uninvolved persons as little as possible, and they should inform the public of the use of drones as far as possible.

Moreover, attempts should be made to blur personal data captured by the drone footage, such as faces and vehicle license plates through automation.

Techniques for and an Example of Depersonalizing Textual Data:

An Example of Depersonalizing Textual Data

Take this example of depersonalization of qualitative textual data provided by the UK's Information Commissioner's Office Anonymisation: managing data protection risk code of practice (2012: 72). All of the changes have been additionally highlighted in the anonymised text. Note how even the information regarding when the interview was done has been altered.

Original text

Interview recorded: 3pm, 10 October 2011

Interviewee: Julius Smith

DoB: 9 September 2005

School: Green Lanes Primary School

I live on Clementine Lane so I walk to school every day. I live in a flat with my parents and my Uncle Jermaine. When I get home from school I watch TV. I don't like reading but I like watching Harry Potter films. My favourite subject at school is art. My teacher is Mr Haines and he is very nice. I used to get bullied by Neil and Chris but I told Mr Haines and they stopped. I play football for Junior Champs, and we are good. I play midfield.

Anonymised text

Interview recorded: October 2011

Interviewee ref: 2011/67

School year: Key Stage 1

School local authority area: Lynenham District Council

I live [in LM51 postcode] so I walk to school every day. I live with [family members]. When I get home from school I watch TV. I don't like reading but I like watching Harry Potter films. My favourite subject at school is art. My teacher is Mr [teacher's name] and he is very nice. I used to get bullied by [other pupils] but I told [the teacher] and they stopped. I play football for [a local team], and we are good. I play midfield

Table 3. Depersonalisation of Textual Data example