

aqua3S Data Protection Notice

Information for the processing of personal data in accordance with art. 14 GDPR

The purpose of this data protection notice is to inform data subjects about the processing of their personal data. Considering the technical nature of the module and limitations imposed by the research design (i.e., scale), it is considered that informing those data subjects directly would involve a disproportionate effort. For this reason, this information is made publicly available via the project's website in accordance with art. 14 GDPR and with its potentially applicable derogations (art. 14 (5) (b) GDPR), as an effort to inform potential data subjects of the data processing and to allow them to exercise their rights. This notice refers to the specific module of aqua3S responsible for collection of data from online sources.

Data will be collected from external online sources, as follows:

- i. **Social Media** (Twitter) & **Call Complaints** in order to capture citizen observations regarding water quality and flood events.

1. The Project

The purpose of aqua3S' research is to enhance standardisation strategies to integrate innovative technologies for safety and security in existing water networks. This research runs from September 2019 to December 2022 and is funded by the European Commission under the Horizon 2020 scheme (grant agreement number 832876). In aqua3S, novel technologies in water safety and security are combined in order to assist professionals to successfully handle and prevent disasters relative to drinking water. Unmanned Aerial Vehicles (**UAVs**) and **CCTV** footage as well as **satellite images** provide various sensor measurements, which are being further complemented by **social media** observations and **Call Complaints** from the citizens that report low-quality water in their area (e.g., by colourisation). In this manner, a holistic overview of the situation is provided to the involved professionals who can later translate this knowledge to actionable insights on how certain situations can be handled or avoided. Through this process, strategies are also being developed to standardize the way these technologies can be incorporated in already existing legacy systems of the water sector. These objectives are being tested and verified in 7 pilot use cases (PUC) in Italy, Bulgaria, Cyprus, Greece, Belgium and France; therefore, data is going to be collected from the aforementioned sources in order to be able to develop the platform and test its capabilities.

2. Key Contacts

The following table provides a detailed list of the primary contacts for aqua3S:

Name	Organisation	e-mail	Role
Dr. Stefanos Vrochidis	CERTH	stefanos@iti.gr	Deputy Coordinator
Spyridon Kintzios	CERTH	sp.kintzios@iti.gr	Coordinator contact

3. Data Processing

The purpose of data collection in this project is to be able to develop the aqua3S project based on the needs and requirements provided by the consortium's end user partners. Within the context of aqua3S' research activities, explicit consent is acquired from the data subjects when it comes to UAVs and CCTV footages collected during the PUCs. These are only used for the aqua3S project within specific locations of interest that are normally not accessible to the public and only for the duration of the research activity. Satellite images are coming from Sentinel-1 and the Sentinel-2 of the Copernicus Open Access Hub which are openly available to the public via the creation of an account to be able to access the API and download the products.

When it comes to the data collected from social media (Twitter) and call complaints though, explicit consent cannot be acquired due to the large amount of data subjects to be contacted and informed individually. This document explains how the aqua3S platform processes personal data from these two sources and applies data protection rights and principles, and in addition to that, within this Data Protection Notice you have been given the contact details of the relevant project representatives (see above 2 Key Contacts) should you have any questions regarding the processing of your personal data.

What personal data is being processed?

The following categories of personal data:

Social Media

- Social media posts (i.e., tweets), including the language, textual content, hashtags, images/videos, whether a post is a retweet or a quote tweet;
- Social media account information, including the username, description (if any from the user), location, as well as the number of friends, followers and favourites;

- Social media user mentions;
- Image links, linked to articles, posts, etc. found on the surface web

Call complaints

- Location (exact coordinates or address) provided by the citizen filing the complaint

No special categories of personal data (art. 9(1) GDPR) will be collected, nor data relating to criminal convictions (art. 10 GDPR). All data will be collected in accordance with the licences and terms & conditions of the data providers. All data will be gathered only from public accounts, with the permission defined by Twitter and in compliance with the respective terms of use, including the ones referred explicitly to the terms of use on behalf of minors, thus in accordance with user expectation of privacy. All collected data will be anonymised, while all user mentions (to other public user accounts) will be visible but not clickable. All data coming regarding the call complaints module are going to be anonymized and given a unique ID number by the partners providing them, except from the location coordinates. Data minimisation will also be applied, i.e., only data that are necessary for the purposes of the project will be processed. Further, details are provided in the “What is the purpose of the processing” section.

What is the purpose of the processing?

The above data will be required: (i) for scientific research purposes, (ii) to facilitate the functionality of other modules of the project, and (iii) for demonstration purposes.

In more detail, as described in the publicly available deliverable D3.6¹: *“The purpose of the [social media crawling] framework is to collect, analyse and finally push the tweets into the aqua3S system. ... Using the necessary credentials, the crawler connects to Twitter Streaming API. The API returns tweets based on keywords that we have set a priori. As a tweet arrives, a four-step analysis is performed in order to identify if it is real or fake (Reliability Estimation), if its image (if any) contains nudity (Nudity Detection) and if it is relevant to the aqua3S use cases (Text Classification). Additionally, we geotag the tweet based on locations (if any) that are mentioned in its text (Geotagging). Then, the tweet along with the extra information of the analysis is stored in a MongoDB database.”*

In regard to the **call complaints** module, the same deliverable (D3.6) reports that two end user partners: *“... have shared an anonymised version of real data, i.e. actual water quality complaints they receive mainly by phone or alternatively by email. In general, when they receive a complaint by phone, they ask for more information and answer directly to the customer. In case they receive an email, depending on the complaint description they*

¹ Available upon request

either answer directly to the customer or contact them to get more information. In both cases, they decide whether it is necessary to take action or not and the complaint is registered in their database”.

Information provided by citizens helps validate the data available through the platform.

Data security

aqua3S and its consortium partners have adopted appropriate technical and organizational measures to ensure an enhanced level of protection against the risks arising from processing personal and non-personal data, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access. Some of these measures include anonymization/pseudonymization techniques; storing of important personal data in secure servers; the access to whom is granted only to people with the “need-to-know”; encryption of data; personal identifiers caught in footages and imagery will be eliminated via crop or blurring before being further processed; interaction with the server hosting the platform will be realized only with secure protocols and only by authorized users; categorization of the data’s visibility per certain user groups in order to ensure that no sensitive information is going to be accessible to people who do not have the “need-to-know”.

Will the collected data be shared?

The collected personal data may be disclosed: (1) to all partners of the Consortium, through a password protected system; and (2) if this is required for the fulfilment of our legal obligations or is necessary for the fulfilment of the above data processing purposes and is in compliance with the applicable legal framework. The information collected will be also used to contribute towards several journal and conference publications as well as scientific contests, in line with Twitter’s Policy. It is also highlighted that no personal data will be transferred outside the European Union (EU) or the European Economic Area (EEA).

Who will be responsible for all of the data when this study is over?

When this study is over, CERTH/ITI will be the only one responsible for the information collected.

How long will data be stored?

The information will be kept for five (5) more years after completion of aqua3S to be available for demonstration in case of an inspection or an audit, or until it is not needed for these purposes anymore.

Will the collected personal data be used for other purposes?

No personal data will be processed for any other purposes outside of those specified in this document.

Will the collected data be processed by automated tools supporting decision-making?

Your personal data will be used to test the capabilities of the aqua3S platform, and you will not suffer any consequences of automated processing supporting decision-making. After hashing your account information, the researchers will not be able to trace back your data to you.

What are your rights?

- *Right to information:* you may request information about whether we hold personal information about you, and, if so, what that information is and why we are holding it. This information shall be provided within a reasonable period after obtaining the personal data, but at the latest within one month.
- *Right to access:* you may request to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- *Right to rectification:* you may ask us to rectify the information that we hold about you in case you consider that something is missing or is incorrect.
- *Right to erasure:* you may ask us to erase your personal data at any given moment without a specific reason.
- *Right to object:* you may request to stop processing delete or remove your personal data at any desired moment where there is no good reason for us continuing to process it
- *Right to data portability:* you have the right to request the transfer of your personal data in an electronic and structured form to another party or directly to you. This enables you to take your data from us in an electronically usable format and to be able to transfer your data to another party in an electronically usable format.
- Lodge a complaint with the Hellenic Data Protection Authority (<https://www.dpa.gr>).

Please note that the aforementioned rights may be restricted in the light of the GDPR (e.g., art. 89 par. 2) or other applicable data protection legislation.

For the exercise of your rights and for any other data-related information you may contact the aqua3S' Deputy Coordinator Dr. Stefanos Vrochidis [stefanos@iti.gr] or/and CERTH'S DPO [dpo@certh.gr]