Deliverable **7.2**

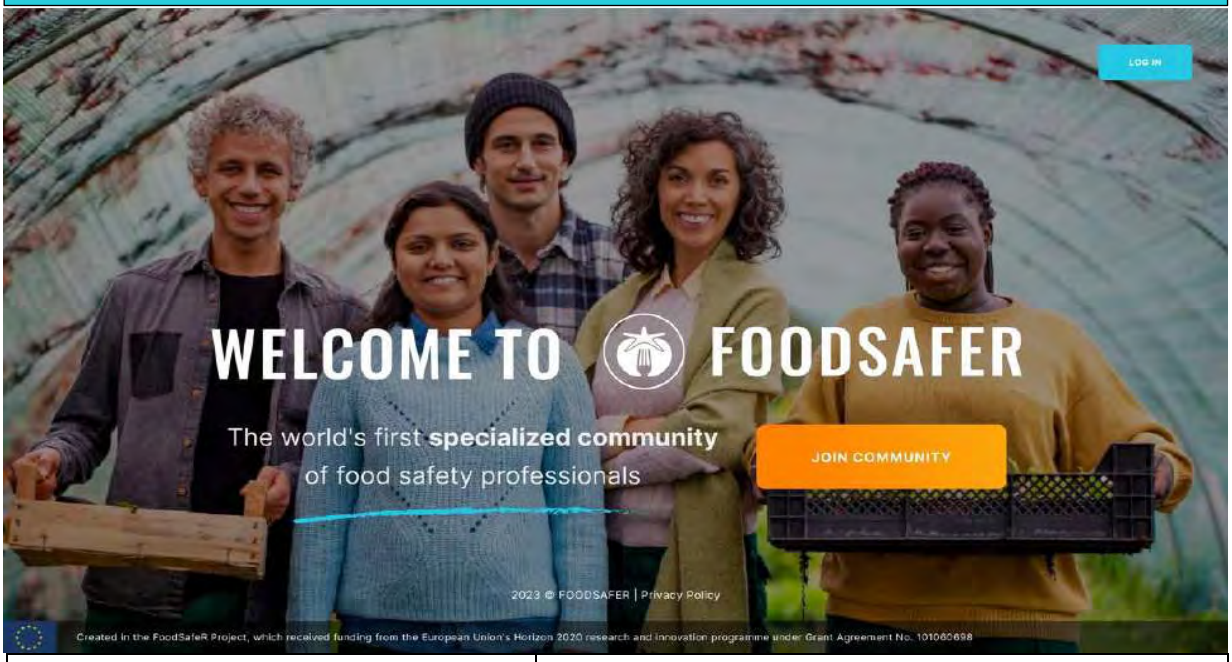
FOODSAFER

OEI Requirements No. 2

#EVERYBODY'S BUSINESS

Ref. Ares(2024)3895839 - 30/05/2024

Deliverable D7.2: OEI Requirement No. 2



Work package number and title	WP7: Ethics requirements
Lead-beneficiary	FFoQSI
Work package Leader	FFoQSI
Contributors to deliverable	External Ethical Advisors
Relevant Task	n.a.
Participants	n.a.
Dissemination Level	SEN (Sensitive)
Due Date (month)	M18 – 31 March 2024

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101060698

Funded by the European Union

1. Introduction

This deliverable targets an assessment on ethical relevance related to the work and results of the FoodSafeR project in reporting period 1 (RP1).

This ethical assessment has been generated by the external ethical advisors that have been appointed at the beginning of the project and named in Deliverable 7.1 "OEI – Requirement No. 1". The external Ethics Advisors for FoodSafeR are:

- Prof. Dr. Herwig Grimm
  (Human-Animal-Interaction / Ethics)

- Prof. Ines Fritz
  (Member of Univ. ethics platform)

As explained within the Ethics Summary Report resulting from the evaluation of the proposal FoodSafeR it has been described that:

The proposal does not raise serious or complex ethics issues however, there are a number of ethics issues that should be considered and dealt with during the life time of the project.
The consortium does not seem to be aware of these ethics issues as they did not flag any ethics issue in Part A of the proposal.
The proposal lacks sufficient detail on how the consortium will address ethics issues related to human participants and the protection of personal data. It is also not completely clear what kind of personal data will be processed from study participants, particularly if any health data will be collected.
Furthermore, ethics issues related to environmental, health and safety are not considered. WP3 involves work with toxic substances such as aflatoxins and alkaloids among others. Some of these compounds are carcinogenic for humans.
Therefore, health risks and safety of the researchers involved in these activities should be accounted for.
An external independent Ethics Advisor should be appointed to assist the consortium at least on the issues related to personal data protection, potential harm caused by the activities of the project on the environment, health and safety of the researchers, participation of non-EU countries and also AI issues.

Based on these requirements the external ethical advisors received the following documents based on reporting period 1 (RP1):

- Progress Report Part B – RP1
- Deliverables RP1
- Description of Work – Part A, B

The FFoQSI management team prepared a questionnaire as support for the ethical advisors to assess these project plans, results and progress on ethical issues.

In addition, a virtual meeting has been organized between the Coordinator and the ethical advisors to brief the advisors and answer related questions.

2. Ethical Assessment

The external ethical advisors answered the following questions related to the FoodSafeR project.

Did you identify any important ethical issues after going through the documents?
Upon scrutinizing the documents, it becomes evident that the project has conscientiously addressed potential ethical considerations in a proactive and well-informed manner. No significant ethical quandaries have been identified because of this meticulous approach.

Are there any environmental, health and safety based ethical issues that you identified?
Based on the humanities and ethical perspective, no particular risks were diagnosed that would go beyond usual good scientific practice.
The advertised forecast model for predicted increased appearance of natural toxins (mycotoxins and plant toxins) will raise severe ethical questions when such a model is intended to be installed and used by authorities. While the outcome is undoubtedly beneficial for general food safety, it must be made clear that no farmer and no region is prejudicated based on model calculation results. Data from deliverables 3.1 and 4.3 fall under this aspect.

Are there any ethical issues related to non-EU countries?
In Deliverable 1.2, it appears necessary to keep an eye on the specific legal situation in the respective countries about "database crawling" – however, the project report shows that the project team is fully aware of this. The same applies to the potential issue of patents, as addressed in Deliverable 4.1.

Are there any ethical issues related to AI topics?
Based on the humanities and ethical perspective, no particular risks that would necessarily be associated with this project were diagnosed in this context.

Data-protection. Check and comment on the use, re-use, and availability of data.
The comprehensive and detailed data management plan indicates a high level of awareness regarding the appropriate handling of data. This assessment is confirmed regarding the individual deliverables. For example: Deliverable D1.1 uses social science methods (literature reviews, expert interviews and documentation and analyses of stakeholder workshops) and provides all essential information on informed consent, anonymization of data or data storage in the documentation.

Objective 4, deliverable 4.3 requires the formulation of a data management plan according to the EU General Data Protection Regulation (Directive 95/46/EC and regulation EU 2016/679) protecting person related data of smartphone app users as well as of those persons which can be identified from the investigated location. Such activities are not mentioned in the current report.

3. Feedback by FoodSafeR consortium

Regarding Objective 4, and the ethical implications of the deployment and use of the Open Digital Hub and related interfaces (web application and mobile applications), a data management plan will be formulated and included in updated version of the project Data Management Plan.

As we are developing a community-based professional digital platform (FoodSafeR Open Digital Hub) focused on the international and European food safety system, we are addressing GDPR compliance, data management, and ethical practices to ensure good compliance and best practices in the operation of the Hub.

General Data Protection Regulation (GDPR) Compliance: As a professional community-based platform, the Hub requires users to register and when they do so they input their name, professional email address and the details of the organisation they work for. To ensure a lawful basis for data processing, explicit consent is obtained from users for collecting, processing, and storing their data. This includes names, professional email addresses, and organizational details. The data is processed for the sole purpose of the functioning of the Hub as a community-based platform. While there is a legitimate interest for processing professional information necessary for platform functionality, but transparency with users is essential. In terms of data **minimisation and purpose limitation**, only the data necessary for platform functionality is collected, which is clearly defined and communicated to users. In relation to **Data Subject Rights**, users can access their data, and also have the ability to correct inaccurate data. We will also provide users with the right to request data deletion (i.e., the "right to be forgotten").

Concerning **data security aspects**, robust security measures are in place to protect personal data, such as data encryption (all transmissions to and from the Hub are encrypted with AES 256_GCM (256 bit) through a TLS 1.3 which is FIPS 140-2 compliant). The production database is based up daily and we have point in time recovery, which means we can recover a database state with a precision of minutes. For the Storage data (files, documents, images...) we save them for 10 days after they have been modified or deleted. Access to the Hub is performed via the following **authentication methods**: Credentials- username (email address) and password; we also support the use of external identity providers, such as Google SSO and Microsoft. Procedures will be in place to regularly update and patch security vulnerabilities, in addition to a protocol for notifying users and relevant authorities within 72 hours of identifying a data breach.

Data Management: Effective data management practices are designed in order to maintaining data integrity, security, and compliance (and which will be updated in the Project Data Management Plan), including: data governance framework outlining data ownership, responsibilities, and access controls; data storage location (in EU and Google Cloud servers located in Germany); data retention policies specifying how long data will be stored and the procedures for secure deletion (as mentioned above, we save data for 10 days after they have been modified or deleted). Regarding data quality, data validation techniques during data entry to minimise errors. In relation to Third-Party Data Integration,

such as the integrations with open-source data, as well as for example the Google Trends alerts, we ensure compliance with the terms of use of these sources. In all integrations, care will be taken to ensure we implement APIs securely to protect data integrity and confidentiality.

Ethical Considerations: Given that the FoodSafeR Open Digital Hub is a professional community-based digital platform it is very important that we carefully and effectively addressing ethical considerations in order to build a responsible, trustworthy and positive professional community. In relation to **transparency and accountability**, as discussed above we maintain transparency about how user data is used and who has access to it, and informed user consent is obtained for data processing activities (and once inside the platform users can modify and control their data settings and preferences). Moreover, we avoid data misuse and ensure data is used for the intended purposes only. A **Code of Conduct** (Code of Practice) is being drawn up outlining acceptable behaviour on the platform, including policies on respectful communication, harassment, and content sharing.