Horizon 2020 Work programme
Food Security, Sustainable Agriculture and Forestry, Marine, Maritime and Inland Water Research and the Bioeconomy
Call
H2020-FNR-2020: Food and Natural Resources
Topic name
FNR-16-2020: ENZYMES FOR MORE ENVIRONMENT-FRIENDLY CONSUMER PRODUCTS

FuturEnzyme:
Technologies of the Future for Low-Cost Enzymes for Environment-Friendly Products
Final ID: 101000327

26/11/2021

ETHICS - POPD - REQUIREMENT NO. 2

D9.2

MANUEL FERRER
CSIC
Marie Curie n2, 28049 Cantoblanco, Madrid, Spain

Document information sheet

Work package:	WP9, Ethics requirements
Authors:	CSIC (Manuel Ferrer, Patricia Molina), ITB (Ilaria Re, Sara Daniotti)
Document version:	1
Date:	26/11/2021
Starting date:	01/06/2021
Duration:	48 months
Lead beneficiary:	CSIC
Participant(s):	CSIC, BSC, Bangor, UHAM, UDUS, IST-ID, CNR, ITB, FHNW, CLIB, Inofea, BioC_Chem, Schoeller, Henkel, Evonik, Eucodis
Dissemination Level:	Confidential, only for consortium's members (including the Commission Services)
Type	Ethics
Due date (months)	6
Contact details:	Manuel Ferrer, mferrer@icp.csic.es

Summary

ETHICS - POPD - REQUIREMENT NO. 2. Description of technical, organisational, and security measures to protect personal data (including contact details of the appointed Data Protection Officer for each partner) and justification for the processing of sensitive personal data

1. Introduction

As part of the engagement on ethics, the FuturEnzyme consortium has been committed to ensure that personal data collected during the project, regardless of the method by which they are collected, will be duly managed, protected and not shared with third parties in accordance with European and national legislation. In particular, all partners of the project and subcontracted third-parties are required to comply with the General Data Protection Regulation (GDPR, Regulation EU 2016/679) as well as specific regulations in the country where they operate.

In this context, this deliverable aims at describing how personal data will be handled during and after the project, describing how the founding principles of GDPR will be followed and the technical, organisational, and security measures developed to ensure the correct personal data management.

Several activities within the project implies personal data collection and processing, mainly contact information to communicate with research participants, receive feedback and implement the follow-up of project activities.

The processing of personal data will be lawful as all research participants will be asked to give their consent for the research purpose only, as it will be detailed in each consent form.

In fact, prior to any of these activities, participants will be informed on the purpose of the activity in which they will be involved and on the kind of information that will be collected and processed. Then, they will be asked for the consent to the processing of personal data in accordance with European and national legislation. The selected subjects can freely decide whether to take part in the research (right to object) and or to withdraw from the survey at any time without any consequences (right to withdraw). The project will ensure to avoid any intentional or unintentional use of information that can bring harm to any participants or being misused in other contexts.

Informed consent procedures and informed consent templates are reported in D9.1 “Report containing the procedures and criteria for recruiting and processing informed consent of the research participants (including consent forms in English)”.

A public event “European Green Deal aligned to Rights, Ethics and Equality” will be organised by FuturEnzyme to reinforce the project’s compromise with a society where ethics as well as gender equality, and rights whatever race, ethnic, and cultural and educational backgrounds are defended and integrated, that are priority EU’s objectives.

In addition, activities or results from FuturEnzyme will not raise security issues nor ‘EU-classified information' as background or results will be involved.

2. Activities that involve personal data collection

2.1. Online survey

Partner involved: ITB

ITB will produce a customer survey based on a Multi-Choice Experiment model by Qualtrics, with at least 10.000 people interviewed across Europe, to understand and analyse how consumers react to these new

enzymes as well as the new products and if they are willing to appreciate and buy the more sustainable enzyme-based products.

Participants will be asked to compare multiple products and select the most attractive in terms of cost, added-value, value of money by responding to simple multi-choice questions.

The survey will collect some personal data, including contact information (name, address, phone number and email address) of the survey respondents; moreover, Qualtrics requires contact information and payment details for customer (ITB in the case of the projects) to provide the customer with access to Qualtrics' services. As part of the survey, additional sensitive data such as gender, income level, and consumer habits will be collected to evaluate whether these factors affect consumers' reactions to the new enzyme-based products. All the data required will be reduced according to the minimisation rule so no more information from the participants that what is strictly needed is provided.

The personal data management and the collection of all questionnaire replies will be entrusted to Qualtrics, an ISO 27001 certified and FedRAMP authorised company. They will manage Personal Data following their Privacy Statement, updated on June 3, 2020, compliant with the GDPR. Qualtrics will provide a final report collecting all the questionnaire replies, further analysed to meet the study objective. However, FuturEnzyme won't receive any respondents' contact information, and the replies will remain totally anonymous for Qualtrics' customers (ITB in this case).

2.2. Product testing

Partners involved: Altroconsumo (subcontracted by ITB)

The product testing will be performed by Altroconsumo, the Italian Consumer Organization, with consolidated experience in tests and investigations on products and services.

Altroconsumo will select 100 consumers from their database and perform a product testing which means that participants will receive a sample of the final products and test them. Altroconsumo's experts will create a set of questions/tests/proofs to be also submitted to the consumers. The audience will be involved in, i.e., interviews, focus groups, surveys (live or online) to ascertain consumer reactions to the project's products. Altroconsumo product test with customers will also involve personal data collection which will be performed according to the GDPR rules and ethical principles[1]. Collected personal data include name, email address, and sensitive data as gender, income level, and consumer habits in order to evaluate whether these factors affect consumers' reactions to the new enzyme-based products. All the data required will be reduced according to the minimisation rule so no more information from the participants that what is strictly needed is provided. The data will be collected, stored, and managed entirely by the subcontractor, who will provide a final report with the main results at the end of the test. Personal data, if collected, will remain confidential and will not be shared with ITB or other project partners.

2.3. Efficacy testing

Partner involved: EVO

EVO will analyse in vivo efficacy properties of enzyme-based cosmetic products. The properties analysed include transepidermal waterloss, skin hydration, overall skin elasticity and wrinkle depth/skin surface replica. Evonik will send an invitation to participate to all their employees on their location so they are free to apply.

As already stated in the Grant Agreement, these tests cannot be considered as clinical studies, in the meaning of the term used for pharma applications. Therefore, WHO or ICMJE approval is not applicable. All tests are performed in a way that no pain or harm can occur, simply because the technology of the tests is in a way of measure with a device that operates only in the surface on the skin (see Annex 2, D9.1).

[1] https://www.altroconsumo.it/info/privacywebinar

During this activity, no personal or health data will be collected from participants; all applicants will remain anonymous. Only if it is necessary, a range of age is asked.

2.4. Demonstration events and teaching activities

Partner involved: CSIC

FuturEnzyme will also consider demonstration events with product prototypes during science festivals and teaching activities with school pupils to implement the communication and dissemination of the project.

As already stated in the Grant Agreement, these activities are regulated by an Agreement signed between the Community of Madrid (General Directorate of Education) and the CSIC, guaranteeing that activities follow ethical principles and that no personal data is collected or shared during the events. A copy if this Agreement is kept, and can be found at the following links:

https://boe.es/boe/dias/2021/10/18/pdfs/BOE-A-2021-16961.pdf

https://www.boe.es/boe/dias/2021/10/19/pdfs/BOE-A-2021-17038.pdf

Moreover, these events do not represent a risk for the attendees since there is no direct contact between the participants and the products.

3. Advisory Board and Panels of Stakeholders, Policymakers and Consumers

In order to strengthen the societal impact of FuturEnzyme activities and products, the project will create a wider network of relevant organizations, platforms and influential individuals, establishing an Advisory Board and Panels of Stakeholders, Policymakers and Consumers.

The project may collect and process personal data from these established panels, mainly contact information to easily communicate with relevant individuals and organizations asking their feedbacks on project activities. The project undertakes to protect personal data from the established Advisory Board and Panels of Stakeholders, Policymakers and Consumers, to respect their confidentiality, and not to share them with third parties, according to European legislation.

4. Transferring personal data to non-EU countries

The project will not collect and process personal data from non-EU countries.

5. European and national legislation on data protection

Every partner performing research activities involving personal data collection will act accordingly to European and national legislation, also taking into account the relevant regulations and protocols at partner's organization.

5.1. European legislation

The main European Regulation on data protection and management is the **Regulation (EU) 2016/679** of the European Parliament of the Council, 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of data, also called **General Data Protection Regulation (GDPR)**[2]. Entered into force on 25 May 2018, it replaced the previous Data Protection Directive 95/46/EC. This new regulation applies to all entities established in the EU that process personal data as part of their activities and entities established outside EU, offering services/goods to individuals in the EU or monitoring the behaviour in the EU of these individuals.

[2] https://eur-lex.europa.eu/eli/reg/2016/679/oj

The GDPR contains a number of new protections for EU citizens and threatens significant penalties for non-compliance. Besides, it provides new security, recordkeeping, access rights, and notification procedures that companies must implement to ensure compliance. Issues that are attracting particular focus include increased administrative requirements, and the need to provide the tools necessary to meet the numerous obligations on both controllers and processors.

Article 4 of GDPR[3] defines **personal data** as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"; according to the same article, **processing** means "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

Personal data shall be processed according to the following principles (defined by article 5 of GDPR[4]):

a) *Lawfulness, fairness and transparency*: "personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject".

   All data collected from human data subjects within the project will require informed consent of the participants engaged in the project. Participants will be duly informed on the purpose of the activity in which they will be involved and on the kind of information that will be collected and processed, giving them all the information to make an informed decision. Therefore, the processing of personal data will be lawful as all research participants will be asked to give their consent for the research purpose. The consortium will also be transparent in the collection of personal data, clearly describing in the consent form and in the related information sheet the kind of information and in what manner it will be collected and processed as well as how this information will be disseminated.

b) *Purpose limitation*: "personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes". The project will not collect any data that is outside the scope of the project. Personal data collected will be limited to reach the aim of each specific activity as defined in section "Activities that involve personal data collection".

c) *Data minimisation*: "personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". Only data that are relevant to the project's aim will be collected. Collecting personal data through multiple-choice and close-ended questions will limit the risk of sharing unnecessary personal data by research participants.

d) *Accuracy*: "personal data shall be accurate and, where necessary, kept up to date". Personal data will be periodically checked for consistency and any misleading or incorrected data will be corrected or, if not possible, erased as soon as possible. To ensure accuracy, personal data will be stored with metadata identifying the source and the timeframe for which the data applies. Respondents have also the right to check the consistency of their personal data and, eventually, ask to modify or complete them if inaccurate.

e) *Storage limitation*: "personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed". All personal data that will no longer be used for project purpose will be immediately deleted. For example, personal emails collected during some project activities to contact research participants will be deleted as soon as they are no longer needed and, in any case, before the ending of the project. Other personal data useful for statistical analysis or for research purpose (for example age,

[3] https://gdpr-info.eu/art-4-gdpr/

[4] https://gdpr-info.eu/art-5-gdpr/

gender, etc…) will be made anonymous as soon as possible or, at least, pseudonymised. At the end of the project, if data has been accurately anonymized, they will be stored in an open repository. Furthermore, in any moment, research participants have the right to access and receive a copy of their personal data collected and stored within the project and, eventually, they have the right to ask for the erasure of their personal data.

f) *Integrity and confidentiality*: "personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing (confidentiality) and against accidental loss, destruction or damage (integrity)". All personal data collected within the project will be handled with appropriate security measures as described in section "Technical, organisational, and security measures to protect personal data".

5.2. National legislation

Spain

- Organic Law 3/2018, of December 5, on Data Protection and Digital Rights Act ("Data Protection Act") entered into force on 7-12-2018 to comply with Regulation 2016/679
- Royal Decree-law 5/2018, of July 27, urgent measures for the adaptation of Spanish law to the European Union regulations on data protection (BOE 183 of 30-07-2018)
- Organic Law 15/1999 on Data Protection and its Development Regulation approved by Royal Decree 1720/2007, of December 21 which implemented the Directive 95/46/EC

National data protection authority: Spanish Data Protection Agency (AEDP)

Italy

- Legislative Decree n. 101 of 10 August 2018 (Amended Personal Data Protection Code) to comply with Regulation 2016/679
- Legislative Decree n. 196 of 30 June 2003 (Personal Data Protection Code) which implemented the Directive 95/46/EC
- Impact assessment on data protection, based on the provisions of the EU Regulation 2016/679 as prescribed by the National Data Protection Authority
- Legislative Decree n. 206/2005 (Consumer Code) on consumer protection

National data protection authority: Italian Data Protection Authority (IDPA or Garante per la Protezione dei Dati Personali)

UK

- Data Protection Act 2018

Germany

- *Bundesdatenschutzgesetz* (Federal Data Protection Act, BDSG) of 30 June 2017. *National data protection authority:* Federal Commissioner for Data Protection and Freedom of Information (BfDI)

Switzerland

- Federal Act on Data Protection (FADP) of 19 June 1992 (Status as of 1 March 2019). https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/en

Portugal

- Data Protection Law No. 58/2019 of 8 August 2019

Austria

- Datenschutzgesetz (DSG) (data protection law) https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597

6. Designation of Data Protection Officer

Articles 37, 38, 39 of GDPR define the designation, the position and the tasks of the Data Protection Officer (DPO).

The primary role of the DPO is to ensure that the organisation processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) is in compliance with the GDPR rules and in cooperation with the data protection authority (EDPS, European Data Protection Supervisor). Therefore, DPO is at the heart of this new legal framework for many organisations, facilitating compliance with the provisions of the GDPR and becoming a competitive advantage for many businesses. In addition to facilitating compliance through the implementation of accountability tools (such as facilitating data protection impact assessments and carrying out or facilitating audits), DPOs act as intermediaries among relevant stakeholders (e.g. supervisory authorities, data subjects, and business units within an organisation). DPOs are not personally responsible in case of non-compliance with the GDPR. The GDPR makes it clear that it is the controller or the processor who is required to ensure and to be able to demonstrate that the processing is performed in accordance with its provisions (Article 24).

The appointment of a DPO must of course be based on her/his personal and professional qualities, but particular attention must be paid to her/his expert knowledge of data protection. A good understanding of the way the organisation operates is also recommended. The DPO can also be external, and in this case, her/his function can be exercised based on a service contract concluded with an individual or an organisation.

In particular, the DPO must:

- Ensure that controllers and data subjects are informed about their data protection rights, obligations and responsibilities and raise awareness about them;
- Give advice and recommendations to the institution about the interpretation or application of the data protection rules.
- Create a register of processing operations within the institution and notify the EDPS those that present specific risks (so-called prior checks).
- Ensure data protection compliance within her/his institution and help the latter to be accountable in this respect.
- Handle queries or complaints on request by the institution, the controller, other person(s), or on her own initiative.
- Cooperate with the EDPS (responding to her/his requests about investigations, complaint handling, inspections conducted by the EDPS, etc.).
- Draw the institution's attention to any failure to comply with the applicable data protection rules.

According to article 37 of GDPR, it is mandatory for certain controllers and processors to designate a DPO. This will be the case for all public authorities and bodies (irrespective of what data they process), and for other organisations that - as a core activity - process data which require regular monitoring of data subject and on a large scale, or that process special categories of personal data on a large scale. Even when the GDPR does not specifically require the appointment of a DPO, organisations may sometimes find it useful to designate a DPO on a voluntary basis. Article 29 Data Protection Working Party ('WP29') encourages these voluntary efforts. Unless it is obvious that an organisation is not required to designate a DPO, the WP29 recommends that controllers and processors document the internal analysis carried out to determine

whether a DPO is to be appointed, in order to be able to demonstrate that the relevant factors have been taken into account properly[5,6].

In the FuturEnzyme Consortium all organizations are obliged by GDPR to appoint a DPO, and this is why all organizations designated/had already designated a DPO on a voluntary basis as listed in **Table 1**, which will be made available to all data subjects involved in the research.

For other beneficiaries not required to appoint a DPO under the GDPR, a detailed data protection policy for the project will be kept on file and submitted to the Agency upon request.

Table 1. Contact/link of the Data Protection Officer/Policy from the institutions conforming FuturEnzyme. The 16 partners of FuturEnzyme have confirmed the appointment of a Data Protection Officer (DPO) from their institution which will be made available to all data subjects involved in the research.

PARTNER	NAME	EMAIL
CSIC	José López Calvo	jose.lopez.calvo@csic.es; delegadoprotecciondatos@csic.es
BSC	-	dpo@bsc.es
BANGOR	Gwenan Hine	gwenan.hine@bangor.ac.uk
UHAM	Dr. Stefan Thiemann	stefan.thiemann@uni-hamburg.de
UDUS	Dr. Ursula Hilgers	datenschutz@hhu.de
IST-ID	Dr. Tiago Silva Abade	rgpd@ulisboa.pt
CNR	Ing. Roberto Puccinelli Dr. Massimo Virgili	rpd@cnr.it massimo.virgili@cnr.it
ITB	Lanfranco Masotti	presidenza@italbiotec.it
FHNW	Karin Hiltwein	Karin.hiltwein@fhnw.ch
CLIB	Dennis Herzberg	herzberg@clib-cluster.de
INOFEA	Anne Timm	anne.timm@inofea.com
BIOC_CHEM	Fabrizio Beltrametti	fbeltrametti@bioc-chemsolutions.com
SCHOELLER	Eveline Scheidegger	eveline_scheidegger@schoeller-textiles.com
HENKEL	-	https://www.henkel.com/data-protection-statement#pageID=9388
EVONIK	-	privacy-policy@evonik.com
EUCODIS	-	office@eucodis.com

7. Technical, organisational and security measures to protect personal data

The management of personal data collected and generated by the survey is entrusted to Qualtrics[7], an ISO 27001 certified and FedRAMP authorised company. ISO 27001 is the international standard that defines the requirements of an information security management system (ISMS), a set of policies, procedures, processes, and systems that manage information risks. Therefore, certification to ISO 27001 demonstrates

[5] Data Protection Working Part. *Guidelines on Data Protection Officers*, 2017: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

[6] https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en

[7] Data Protection & Privacy (qualtrics.com)

that Qualtrics has defined and put in place best-practice information security processes[8]. Qualtrics is also FedRAMP Authorized. FedRAMP is the standard of U.S. government security compliance, with over 300 controls based on the highly regarded NIST 800-53 that requires constant monitoring and periodic independent assessments.

To ensure full protection of collected data, Qualtrics provides technology that enables its customer to be compliant with GDPR and other privacy laws. According to Qualtrics' security statement, Qualtrics' servers are protected by high-end firewall systems and scans are performed regularly to quickly find and patch any vulnerabilities. Application penetration tests are performed annually by an independent third-party. All services have quick failover points and redundant hardware, with backups performed daily.

Access to systems is restricted to specific individuals who have a need-to-know such information and who are bound by confidentiality obligations. Access is monitored and audited for compliance.

Qualtrics uses Transport Layer Security (TLS) encryption (also known as HTTPS) for all transmitted data. Surveys may be protected with passwords. Qualtrics' services are hosted by trusted data centres that are independently audited using the industry standard SSAE-18 method[9].

Brand administrators can permanently delete individual contacts and respondent personal data if a data subject request it, answering its right to be forgotten. Qualtrics one-touch data deletion functionality means erasure happens in one place, with just a few clicks, making easier to respond to data subject requests[10].

For Altroconsumo, the Joint Controllers adopt adequate technical and organizational security procedures and measures to ensure the safe processing of personal data, such as the imposition of confidentiality obligations on their collaborators and suppliers; the limitation of access to personal data; or the destruction or anonymisation of personal data if no longer necessary for the purposes for which they were collected.

Since information security depends in part on the security of the computer or device used to interact with the Joint Controllers and on the security adopted to protect (if applicable) user names and passwords, data subjects are asked to pay particular attention to how this data is obtained keep them.

No other partner considers to organize a consumer survey with personal data collection and therefore no management of personal data is planned.

8. Contacts for Ethics Committees of the partners

Table 2. Contact/link of the responsible of the Ethics Committee from the institutions conforming FuturEnzyme.

PARTNER	NAME	EMAIL
CSIC	D. Lluís Montoliu José	montoliu@cnb.csic.es; comitedeetica@csic.es
BSC	Simona Giardina[1]	simona.giardina@bsc.es
BANGOR	Gwenan Hine	gwenan.hine@bangor.ac.uk
UHAM	-	https://www.inf.uni-hamburg.de/en/home/ethics.html
UDUS	Prof. Dr. med. Thomas Hohlfeld	ethikkommission@med.uni-duesseldorf.de
IST-ID	-	comissaoetica@tecnico.ulisboa.pt
CNR	Dr. Cinzia Caporale	cnr.ethics@cnr.it
ITB	Lanfranco Masotti	presidenza@italbiotec.it
FHNW	Karin Hiltwein	Karin.hiltwein@fhnw.ch

[8] https://www.itgovernance.co.uk/iso27001-benefits
[9] https://www.qualtrics.com/security-statement/
[10] https://www.qualtrics.com/uk/platform/gdpr/

CLIB	Dennis Herzberg	herzberg@clib-cluster.de
INOFEA	Anne Timm	anne.timm@inofea.com
BIOC_CHEM	Fabrizio Beltrametti	fbeltrametti@bioc-chemsolutions.com
SCHOELLER	Eveline Scheidegger	eveline_scheidegger@schoeller-textiles.com
HENKEL	-	https://www.henkel.com/sustainability/positions/white-biotechnology
EVONIK	-	compliance-officer@evonik.com
EUCODIS	Jan Modregger	modregger@eucodis.com

[1]Secretary of the BSC Internal Board of Revision of projects, in collaboration with BSC experts and legal and DPO departments.