REACH

NEXT GENERATION DATA INCUBATOR

ETHICAL GUIDELINES FOR SUBGRANTEES

REACH 3rd open call for proposals

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 951981

CORE PARTNERS

DATA PROVIDERS

Introduction

This document is based on the "EU Grants: How to complete your ethics self-assessment" version 2.0 published on the 13th of July of 2021 by the European Commission.

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 951981

CORE PARTNERS

DATA PROVIDERS

Table of Content

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 951981

CORE PARTNERS

DATA PROVIDERS

1 PROHIBITED ACTIVITES

Subgrantees are forbidden to carry out the following activities in the context of the REACH Project:

1. Activities involving the use, production or collection of human cells and/or tissues (including embryonic stem cells and human embryos).
2. Activities involving the work with human beings that are not part of the applicant's staff and that belong to potentially vulnerable groups, such as children, patients, people subject to discrimination, minorities, people unable to give consent, sex workers, etc.
3. Activities involving animal testing.
4. Activities which may adversely affect the environment and/or the health and safety of the persons involved.
5. Activities which are prohibited in the EU even though they may be carried out in a non-EU country.

In consequence, proposals which involve these kinds of activities will be considered ineligible within the evaluation process and therefore excluded from the participation in the REACH Project.

2 PROJECT INVOLVING HUMANS

This section refers to projects with activities involving work with human beings that are not part of the staff of the Subgrantees. It thus covers research or study participants, persons concerned by the project activities, etc., regardless of its nature or topic.

- Common to all fields, the main ethics issues concern:
- The respect for persons and for human dignity.
- Fair distribution of benefits and burden.
- The rights and interests of the participants.
- The need to ensure participants' free informed consent (with particular attention to vulnerable categories of individuals such as children, patients, discriminated people, minorities, persons unable to give consent, etc.).

Moreover, the methodologies Subgrantees use should not result in discriminatory practices or unfair treatment.

If your project involves work with human beings you must:

a) Comply with the highest ethical standards.

b) Comply with applicable international, EU and national law.

c) Gather the participant's previous free and fully informed written consent. Participants must be given a project-specific informed consent form and detailed information sheets that:

- are written in a language and in terms they can fully understand.
- describe the aims, methods and implications of the project activity, the nature of the participation and any benefits, risks or discomfort that might ensue.
- explicitly state that participation is voluntary and that anyone has the right to refuse to participate and to withdraw their participation or data at any time — without any consequences.

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 951981

CORE PARTNERS

DATA PROVIDERS

- state how data will be collected, protected during the project and whether it will be destroyed or reused afterwards.
- state what procedures will be implemented in the event of unexpected or incidental findings (in particular, how and when participants will be informed about such finding, whether they have the right "not to know" about any such findings, and whether relevant findings.

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

Ensure that any personal data are kept securely and that publication of aggregate or anonymized data (including publication on the internet) does not lead (either directly or indirectly) to a breach of agreed confidentiality and anonymity.

Data collection using electronic encoding tools (digital recorders or cameras) should be given special attention. You should also discuss these issues with your organisation's data protection officer.

3 PERSONAL DATA

This section concerns projects with research activities that involve processing of personal data, regardless of the method used (e.g. interviews, surveys, questionnaires, direct online retrieval etc.).

Personal data — Information relating to an identified or identifiable natural person.

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 (Article 2(a) EU General Data Protection Regulation 2016/679 (GDPR)).

Individuals are not considered 'identifiable' if identifying them requires excessive effort.

Completely anonymised data do not fall under the data protection rules (as from the moment it has been completely anonymised, the GDPR is not applicable).

Special categories of personal data (formerly known as 'sensitive data') — Include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (Article 9(1) GDPR).

The processing of such data is subject to more stringent data-protection safeguards. Member states may introduce special derogations/limitations with regard to the processing of genetic, data, biometric data and data concerning health.

Personal data related to criminal convictions and offences — Can be only processed under the control of official authorities or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects (Article 10 GDPR).

The processing of personal data by state authorities for law enforcement purposes is governed by EU Directive 2016/680.

Processing of personal data — Any operation (or set of operations) performed on personal data, either manually or by automatic means. This includes:

- collection (digital audio recording, digital video caption, etc.)
- recording
- organisation, structuring and storage (cloud, LAN or WAN servers)

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 951981

CORE PARTNERS

DATA PROVIDERS

- adaptation or alteration (merging sets, appification, etc.)
- retrieval and consultation
- use
- disclosure by transmission, dissemination or otherwise making available
- (share, exchange, transfer)
- alignment or combination
- restriction, erasure or destruction.

In research, data processing normally covers any project that uses data for research purposes (even if interviewees, human volunteers, patients, etc. are not actively included in the research).

Personal data may come from any type of research activity (ICT, genetic sample collection, tissue storage, personal records (financial, criminal, education, etc.), lifestyle and health information, family histories, physical characteristics, gender and ethnic background, location tracking and domicile information, etc.).

Your research activities must comply:

- The highest ethical standards
- Applicable international, EU and national law (in particular, the GDPR, national data protection laws and other relevant legislation).
- Under these rules, personal data must be processed in accordance with certain principles and conditions that aim to limit the negative impact on the persons concerned and ensure fairness, transparency and accountability of the data processing, data quality and confidentiality.

This implies the following main obligations:

- Data processing should be subject to appropriate safeguards (see table above).
- Data should wherever possible be processed in anonymised or pseudonymised form.
- Data processing is subject to free and fully informed consent of the persons concerned (unless already covered by another legal basis, e.g. legitimate or public interest).
- Data processing must NOT be performed in secret and participants/data subjects must be made aware that they take part in the project and be informed of their rights and the potential risks that the data processing may bring
- Information about the data processing operations and the contact details of the data protection officer (project DPO or partner DPO, whichever relevant) must be provided to the participants (art 13/art 14 GDPR).
- Data may be processed ONLY if it is really adequate, relevant and limited to what is necessary for the project ('data minimisation principle').
- Collecting personal data (e.g. on religion, sexual orientation, race, ethnicity, etc.) that is not essential to your project may expose you to allegations of hidden objectives or mission creep (i.e. collecting information with permission for one purpose and using it/making it available — online or otherwise — for another reason, without additional permission).
- Data processing operations which are more intrusive and likely to raise higher ethics risks must be subject to higher safeguards.
- For complex, sensitive or large-scale data processing or data transfers outside of the EU, you should consult your data protection officer (DPO), if you have one, or a suitably qualified expert.
- The level of data security must be appropriate to the risks for the participants/data subjects in case of unauthorized access or disclosure, accidental deletion or destruction of the data.
- You are responsible for all your partners, contractors or service providers that process data at your request or on your behalf.

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 951981

CORE PARTNERS

DATA PROVIDERS

Generally, one of the best ways how to avoid/limit data protection issues for your project is to use anonymised or pseudonymised data.

Pseudonymisation and anonymisation are not the same thing.

'Anonymised' means that the data has been rendered anonymous in such a way that the data subject can no longer be identified (and therefore is no longer personal data and thus outside the scope of data protection law).

'Pseudonymised' means to divide the data from its direct identifiers so that linkage to a person is only possible with additional information that is held separately. The additional information must be kept separately and securely from processed data to ensure non-attribution.

Moreover, if you have a data protection officer (DPO), it is generally recommended to involve them in all stages of your project, whenever it comes to privacy and data protection issues, since this will help your proposal and grant implementation (EU grants are subject to full compliance with privacy and data protection rules).

Be aware that even if you solve all privacy-related issues, data may still raise other ethics issues, such as potential misuse of methodology/findings or ethics harms to specific groups.

4 ARTIFICAL INTELLIGENCE

This section concerns projects with activities involving the development, deployment and/or use of artificial intelligence (AI)-based systems or techniques.

The manner in which an AI solution is deployed or used may change the ethical characteristics of the system. It is therefore important to ensure ethics compliance even in cases where your project does not develop itself an AI based system/technique.

A Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)9 is currently pending adoption by the EU legislator. This Regulation, when it enters into force, may have effect on your project activities.

Before its adoption and entry into force, the Subgrantees must use the Ethics Self-assessment for applicants to develop procedures to detect, assess the level and address potential risks.

Your activities must comply with the:

- Highest ethical standards.
- Applicable international, EU and national law (in particular, the principles and values enshrined in the EU Charter of Fundamental rights and the EU Treaties).

This requires specific ethically-focused approach during the development, deployment, and/or use of AI-based solutions.

Any use of AI systems or techniques should be clearly described in the project and you must demonstrate their technical robustness and safety (they must be dependable and resilient to changes).

The approach must be built upon the following key prerequisites for ethically sound AI systems:

- Human agency and oversight — AI systems must support human autonomy and decision-making, enabling users to make informed autonomous decisions regarding the AI systems. This is particularly relevant for AI systems that can affect human behaviour by guiding, influencing or supporting humans in decision- making processes (e.g. recommendation systems, predictive algorithms, disease diagnosing tools). The right to human agency should be safeguarded by setting up appropriate oversight mechanisms to prevent possible adverse effects and uphold human autonomy.

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 951981

CORE PARTNERS

DATA PROVIDERS

AI systems must not subordinate, coerce, deceive or manipulate people, and should not create attachment or stimulate addiction.

- Privacy and data governance — AI systems must guarantee privacy and data protection throughout the system's lifecycle. The principles of privacy by design and by default must be taken into account in the process of designing, developing, selecting and using AI. The quality, integrity and security of data should be rigorously checked and adequately managed. Data minimisation and data protection should never be leveraged to hide or obscure bias, and these should be addressed without harming privacy rights
- Transparency — All data sets and processes associated with AI decisions must be well communicated and appropriately documented. AI systems must be explainable and open in the communication about their limitations. The principle of transparency is closely linked to the principles of tractability and explicability and facilitates the implementation of human agency, data governance and human oversight. It includes all elements relevant to an AI system (e.g. the data, the system and the processes by which it is designed, deployed and operated).
- Fairness, diversity and non-discrimination — Best possible efforts should be made to avoid unfair bias (e.g. stemming from the used data sets or the ways the AI is developed). AI systems should be user-centric and whenever relevant, designed to be usable by different types of end-users with different abilities. AI systems should avoid functional bias by offering the same level of functionality and benefits to end-users with different abilities, beliefs, preferences and interests, to the extent possible. Inclusion and diversity must be enabled during the entire life cycle of the AI system. Use diverse design teams and ensure participation of affected stakeholders to ensure objectivity and inclusiveness of the developed systems/approaches.
- Societal and environmental well-being — The impact of the developed and/or used AI system/technique on the individual, society and environment must be carefully evaluated and any possible risk of harm must be avoided. Increased vigilance is needed for solutions that may potentially have significant negative social or environmental impact. Sustainability and ecological responsibility of AI systems should be encouraged, and research should be fostered into AI solutions addressing areas of global concern, for instance the Sustainable Development Goals. Overall, AI should be used to bring positive transformative changes to the society, environment or the economy. AI systems should serve to maintain and foster democratic processes and respect the plurality of values and life choices of individuals; they must not undermine democratic processes, human deliberation or democratic voting systems or pose a systemic threat to society at large.
- Accountability — Requires that the actors involved in their development or operation take responsibility for the way that these applications function and for the resulting consequences. Accountability requires presupposes certain levels of transparency as well as oversight. To be held to account, developers or operators of AI systems must be able to explain how and why a system exhibits particular characteristics or results in certain outcomes.

This implies that, amongst others, the developed/used AI solutions must:

- Ensure that people are aware they are interacting with an AI system and are informed (in a language and terms understandable by all) about its abilities, limitations, risks and benefits. The manner in which this is done must be described in the proposal.
- The manner in which information is provided should not depend on particular educational backgrounds, technical knowledge, or other skills which cannot be assumed of all people.
- Prevent possible limitations on human rights and freedoms (e.g. freedom of expression, access to information, freedom of movement etc.).
- Not be designed in a way that may lead to objectification, dehumanization, subordination, discrimination, stereotyping, coercion, manipulation of people or creation of attachment or addiction.

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 951981

CORE PARTNERS

DATA PROVIDERS

- Be able to demonstrate compliance with the principles of data minimisation and privacy by design and by default when processing personal data. The principles of lawfulness, transparency and fairness of the data processing must be respected at all times. For more information, please consult the Guidance on ethics and data protection in research projects.
- Must be designed in a way to avoid bias in both input data and algorithm design. The systems should be able to prevent potential discrimination, stigmatisation or any other adverse effects on the individual related to the use of the developed/deployed AI system/technique. The manner in which this is done must be described in your project proposal.
- Must address the potential impact on the individual, society or the environment. An evaluation of the potential negative individual, societal and/or environmental impacts must be carried out and be included in the project proposal along with the measures to be set in place to mitigate any potential adverse effect.
- The ethics risk assessment and risk mitigation measures must cover the development, deployment and post-deployment phases.
- Must not reduce the safety and wellbeing of the individuals. Whenever relevant, the safety of the developed/used systems must be demonstrated in the project proposal
- Should be developed in a way that enables human oversight (human-in-the- loop, human-on-the-loop, human-in-command), traceability and auditability. Whenever possible, explanation on how decisions are taken by the developed/used AI along with the logic behind it should be provided to the users.

For further detailed requirements, please consult the Ethics self-asessment for applicants.

At the development stage, the implementation of the key requirements for ethically sound AI systems can be ensured by adopting the 'ethics by design' approach. The latter is aimed at preventing ethics issues from occurring by integrating ethics values- based requirements into the design of the developed/used AI solution. The ethics by design approach will greatly facilitate your ethics compliance. For more information, please consult Guidelines on ethics by design for AI.

Some types of objectives, methodologies, system architecture or design may be inherently problematic (due to serious ethical non-compliance). This is the case for instance for AI systems that risk to:

- Limit human rights, subordinate, deceive or manipulate people, violate bodily or mental integrity, create attachment or addiction, or hide the fact people are interacting with an AI system.
- Cause people to be disadvantaged socially or politically, reduce the power that they have over their lives, or result in discrimination, either by the system, or by the way it will be used.
- Cause people to suffer physical, psychological or financial harm, cause environmental damage, or significantly damage social processes and institutions (for example, by contributing to misinformation of the public).

For all issues related to the involvement of humans, data protection, safety and environmental impacts, please consult the relevant sections of this guidance.

5 POTENTIAL MISUSE OF RESULTS

This section concerns projects with activities that involve or generate materials, methods, technologies or knowledge that could be misused for unethical purposes.

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 951981

CORE PARTNERS

DATA PROVIDERS

Although projects are usually carried out with benign intentions, they may have the potential to harm humans, animals or the environment.

To identify any possible misuse, start by considering the risks associated with the activities you plan and any unethical ways in which the materials, methods, technologies and knowledge involved could be used.

Activities most vulnerable to misuse could include:

- The development of surveillance technologies that could curtail human rights and civil liberties.
- The involvement of minority or vulnerable groups or the development of social, behavioural or genetic profiling technologies that could be misused to stigmatise, discriminate against, harass or intimidate people.
- The development of materials/methods/technologies and knowledge that could harm humans, animals or the environment if they were released, modified or enhanced.
- In general, the development of materials/methods/technologies and knowledge that could serve purposes other than those intended, and if so, in unethical ways.

This guide does not cover research misconduct (e.g. falsification of research results, fabrication of scientific evidence and plagiarism).

Some questions that could be used to identify potential misuse are:

- Could the materials/methods/technologies and knowledge involved or generated harm humans, animals or the environment if they were modified or enhanced?
- Could the materials/methods/technologies and knowledge involved or generated serve purposes other than those intended? If so, would such use be unethical?

There are various ways to mitigate risk. Depending on the activity planned and the potential misuse, applicants may choose to:

- Take additional safety measures, e.g. compulsory safety training for staff.
- Adjust the project design, e.g. use dummy data.
- Limit dissemination, e.g. by publishing only part of the results, regulating export, etc.
- Appoint an independent ethics advisor or an ethics advisory board with experts from different backgrounds.

If you are planning activities that may give rise to concerns about potential misuse, you will need to do the following when preparing your proposal:

- Provide a risk-assessment and explain how you will prevent misuse.
- If required, attach copies of health and safety authorisations, and ethics approvals if relevant.
- Details on applicable international, EU and national laws that address concerns relating to potential misuse of materials/methods/technologies and knowledge that could harm humans, animals or the environment if they were released, modified or enhanced.

Specific cases

Activities with a potential impact on human rights — Concerns in this field relate primarily to surveillance technologies, new data-gathering and data-merging technologies (e.g. in the context of big data). However, social or genetic research that could lead to discrimination or stigmatisation is also affected.

Risk mitigation measures may include:

- A human rights impact assessment.
- Involving human rights experts in your project.

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 951981

CORE PARTNERS

DATA PROVIDERS

- Training personnel and/or technological safeguards.
- Caution when publishing or otherwise disseminating results (e.g. through privacy by design).
- Adapting the project design (e.g. using dummy data).

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 951981

CORE PARTNERS

DATA PROVIDERS