OActive

Project Title:

Advanced personalised, multi-scale computer models preventing osteoarthritis

SC1-PM-17-2017 - Personalised computer models and in-silico systems for well-being

General ethics, data protection and safety manual for EU funded projects

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 777159

Table of Contents

1 General ethics, data protection and safety manual for EU funded projects

The purpose of this manual is to briefly present an overview of the actions to take to achieve compliance with general ethics, data protection and safety requirements in EU funded projects. While ethics and data protection challenges will of course vary from project to project, the most common ethics, and data protection challenges to address in the frame of a research project are briefly commented as well.

As a practical note, this note does not examine legal compliance requirements in detail. While high level priorities and actions are defined to support data protection compliance (notably in relation to the GDPR), this manual is not a substitute for appropriate legal diligence.

2 Implementations check list

While each project is of course different, the general approach to facilitating ethics, data protection and safety compliance can be generalised to some extent. The following overview can be used as a step-by-step list in organising compliance in various stages of the project.

STEP 1. Initial identification of ethics and safety objectives and values

The first step is to identify the core ethical requirements for the execution of the project, without at that stage delving deep into operational implementation. The purpose is to identify the European ethical values that are at the centre of the project: what is the benefit that it aims to achieve, who could be affected positively or negatively, and what are the trade-offs that might occur (including conflicts of ethical values)? The goal is not to resolve problems, but to draw ethical lines and imperatives that will help to address ethics and data protection requirements, and requirement liked to the participation of real persons to the projects. The result of the process should be formalised in a short ethical policy statement for the project, which is shared with and supported by all partners, and which includes a mechanism for escalating and discussing future ethics problems.

This step should be completed in the first months of the project. The compliance objectives list in Annex I may be a useful starting point for this first step.

STEP 2. Early mapping of data flows and identification of parties involved

The purpose of this step is to identify the data cycles in the project, as they are understood by the partners at the beginning of the project: where does the data come from, what is it used for and by which partner; where is the data stored, for how long and under which modalities?

The aim is to establish a good overview of data collection, exchange and use practices, both for supposedly trivial activities (e.g., project communications, shared spaces, workshops, surveys, …) and for more complex activities (clinical trials, social science research, AI analytics, deep learning, profiling, etc). This should match (or at least build on) with the description of work of the project.

Based on this input, the responsibilities of all partners should be identified, discussed, and accepted, based on their actual activities throughout the action. The role and qualification of any service providers (e.g., cloud service provider) must be considered as well in relation to the consortium as it may require further action.

During this stage at the latest, the project should also assess whether it needs to appoint one or more data protection officers (DPOs) under EU data protection law and identify which of the partners have a DPO

(whether this is legally mandatory or not). An overview should be established of any DPOs, including their contact information (e-mail addresses at a minimum). This will facilitate the resolution of any data protection compliance challenges.

This step should be completed in the first months of the project. The result is generally tentative and will evolve significantly over time. This is not a problem; however, it is important to establish an early overview of plans and assumptions, since these strongly affect ethics risks.

The output of this step will be maintained as will be explained in Step 4 below; and can also feed into any Data Management Plan required under the project.

STEP 3. Data protection impact assessment (where necessary)

A data protection impact assessment (DPIA) is a formal activity, the purpose of which is to demonstrate the implementation of data protection principles. DPIAs are mainly performed when processing personal data as defined under EU data protection law (including the GDPR).

In principle, a DPIA must be carried out when a data processing activity is expected to result in a high risk to the rights and freedoms of natural persons, considering the nature, scope, context, and purposes of the processing, and when using new technologies. Additionally, when the processing supposes either the systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and resulting legal effects concerning the natural person or similarly significantly affect the natural person or, the processing on a large scale of sensitive data or, the systematic monitoring of a publicly accessible area on a large scale, the performance of a DPIA is required. Due to the 'new technologies' criterion, DPIAs are often (but not always) mandatory in EU research projects that focus on personal data.

The DPIA should be performed before the processing of personal data begins. For that reason, a DPIA should precede any piloting activities or data collection being done in the context of a project. A DPIA is however an iterative action: it should be initially performed before the piloting/research activities begin and updated periodically to account for any modifications or lessons learned following the testing phase. It is strongly recommended to re-use established and publicly available tools, rather than inventing a new methodology.

The aim of a DPIA is to assess the risks on the fundamental rights and freedoms of a data subject. Such risks, in a data protection perspective are encountered when personal data are accessed, modified, or deleted in an unauthorized manner. Hence, when performing a DPIA you should evaluate the likelihood of such risks materializing, and how severely the persons concerned would be impacted. Risk mitigation measures should be defined, and a process should be defined to address any problems or incidents that emerge. A DPIA should be performed alongside or in tandem with a risk assessment normally performed when developing new processes and new devices.

STEP 4. Implementation of compliance measures and monitoring compliance

The purpose of this step is to define, based on the output from the previous steps, and implement the controls necessary to comply with the ethics objectives and values defined earlier.

a. Ethics and data protection governance

The main ethics challenge in any research project is communication and awareness. It is imperative that a mechanism is set up that enables, encourages, and even requires all project partners to flag ethics issues (including data protection compliance problems) so that they can be discussed and resolved. This requires

the identification of a contact point, clear drafting, and dissemination of a concise ethics requirements policy statement (see step 1), and frequent repetition of the importance of ethics and data protection. The goal is to ensure that good faith ignorance of these issues is not possible.

b. Definition and implementation of security and safety measures

It is important (and required when dealing with personal data) to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk identified. The definition of the measures must consider the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

The measures should ensure the security of personal data as required under data protection law but should also ensure the general safety of the project's execution. This includes e.g. measures to mitigate any risks of personal injury or physical damage.

These measures should be documented in a written form, i.e., in one or more policies. It is not required (nor appropriate in most cases) that a single policy covers all partners in the same way, since the policies should be relevant to the risks, which may differ widely. Similarly, it is not required (even though it is recommended) that the policies are shared among all partners. The main requirement is that the policies exist and fit for purpose. If a partner can satisfy this requirement on its own, this can be acceptable.

c. Information notices and transparency

Under EU data protection law, data subjects have the right to be informed of the processing of their personal data. This can be achieved verbally during the data collection, or in written format before or during the collection. This presupposes the preparation of information notices explaining (among other points) why and how personal data will be processed, by whom, and what the rights of the data subjects are. This information can be merged with more general information provided to pilot/ research participants where relevant. It is good practice to keep this information available at all time for the data subjects, by posting it on the website of the project, and providing a link to it in any communication with the participants.

Notices can be standardised across the project activities, but the central goal is that transparency is ensured. This often requires tailoring, not only for linguistic reasons, but also to address the audience in a language that they can understand. A notice that seems to contain all legally required elements, but which cannot be reasonably understood by the target audience is not ethically sound.

d. Consent process

Consent can play an important role in organising participation in research activities. It can serve as a legal basis for the collection and processing of personal data in some cases, or act as a procedural requirement, or merely be used as an ethical safeguard.

When a project relies on consents, the consent process for participation in the research must be defined in advance between the partners. After identifying the relevant partner in charge of gathering consents, the information to provide must be defined, taking in consideration legal and ethical requirements, as well as the technical needs of the project. It must be abundantly clear to the pilots' participants what they are consenting to, and that they may withdraw at any time, without negative consequences. The consent process must account for the possibility that participants may withdraw. An appropriate process for this eventuality must be prepared in advance.

Consent may be oral or in written format, but it must always be demonstrable, i.e., proof of consent must be available. Therefore, the consent obtained must be stored, preferably separately from the collected data. This is an ethical and compliance requirement.

e. Record of all data processing activities, including incidents and complaints

The maintenance of a record of processing activities is an obligation under the GDPR. The record must be kept in writing, and provide basic information of the processing activities undertaken, including the legal role of partners involved (either as controllers or processors under EU data protection law).

It is recommended to establish a shared record of processing activities for the project collectively (e.g., on a shared workspace), since this allows all participants to keep an overview of processing activities, and to object when they see anomalies (e.g. when they are designated as legally responsible for a data processing activity when they did not accept this role, or when they see that their data is stored in a location that they did not approve of).

Complaints in relation to data processing activities should be stored as well, and an overview should be kept of incidents, including any data breaches, along with the actions taken by the relevant project partners and the justification of these actions.

f. Privacy policy for the project website

The project website is the primary means to dissemination and communication of the outcome of the project, as well as a first point of contact with the consortium. Therefore, the project website must have a privacy policy covering at least the possible contact with the consortium, through the website, but also conferences and workshop, as well as other activities of the consortium that may require the processing of personal data for the purpose of the project, such as surveys, or monitoring the visits of the website though the use of cookies, or social media pages of the project and integration of social media plug-ins.

g. Contractual measures

Under European data protection law (including the GDPR), most exchanges of personal data (whatever the reason) will require the conclusion of formal agreements. These should be drafted in advance. Note that the Grant Agreement and Consortium Agreement for an EU funded project will virtually never be sufficient to satisfy these requirements, and separate agreements are almost always necessary.

i. Data transfer/ sharing agreements

Based on the identified data flows, you should make sure that any access to re-use of pre-existing data sets is properly organised. If the access is dependent on a data transfer agreement, or any other contractual agreement, you should check for discrepancies between the authorised uses of the data set and the purposes of the project and verify the adequacy of safeguards in place.

ii. Joint-controllers agreement

When project partners jointly decide on the purposes and means of collected personal data, you should prepare a joint controller agreement to transparently determine their respective responsibilities for compliance with the obligations under GDPR, notably as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14 of the GDPR. The essence of the arrangement must be made available to the data subjects.

iii. Data processing agreement

When a party processes data on behalf of another party, a data processing agreement should be prepared. A Data Processing Agreement is required by article 28 of the GDPR. It outlines the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller, as well as the measures to implement concerning the data processed upon termination of the agreement. An EU funded template for such an agreement can be found at https://gdpr.eu/data-processing-agreement/

STEP 5. Project termination and (if applicable) sustainability strategy

a. Determine what will be done with the data, including how long it will be kept and by whom

Before the project ends, you should evaluate the possible use for the data gathered and/or produced throughout the project, whether it needs to be retained, and what it would mean in term of storage duration, and security measures to implement. Any decision on this point needs to be formalised. Note that simple deletion of all collected data is often not legally possible, since partners will typically need to retain proof for a certain period of time that they implemented the project appropriately. Naïve policies promising global deletion of all collected data therefore need to be carefully considered.

b. If open access – anonymisation strategy

Depending on the funding scheme, the Consortium may have various obligations concerning Open Access to project results. Notably scientific publications made for dissemination purposes must in principle be made available free of charge online for any user. This obligation also covers the research data needed to validate the findings of the scientific publication. Indeed, the partners have the obligation to make the research data and the associated metadata available for access, mining, exploitation, reproduction, and dissemination. This cannot be done for personal data without corrective and mitigating measures that protect the persons concerned against unlawful use of their data. Therefore, the partners must define an anonymisation strategy for any personal data, balancing the need of future research project and the privacy of the data subjects. When data cannot be effectively anonymised without destroying its usefulness, a conditional access process must be defined where data can be accessed only after appropriate verifications.

c. Project closure - checking legacy systems and project repositories

Throughout the project you may have used service providers external to the consortium to store and otherwise process data. The service providers are processors, and therefore may not keep the data once the processing is no longer necessary. You should ensure the data is either deleted or transferred back to you, or to an archiving service covered by appropriate agreements. This should be organised in the data processing agreement signed between the controller and the service provider.

3 Annex I - Compliance objectives

The objectives cover the fundamental requirements a research project should comply with, in terms of research ethics and data protection. The objectives should always be tailored to the project to ensure their relevance. The list in this Annex has been identified based on the analysis of applicable relevant legislation at the EU level, including notably the EU Charter of Fundamental Rights, the General Data Protection Regulation (EU) 2016/679 (as the core document in the EU on data protection and informational privacy protection, including for data concerning health), and the Clinical Trials Regulation (EU) 536/2014 (as the core document on clinical trials, including patient rights and safety issues).

Non-legislative policy and guidance documents have also been considered, notably the FP7 Data protection and privacy ethical guidelines, the Opinion of the European Group on Ethics in Science and New Technologies on the ethical implications of new health technologies and citizen participation, the World Medical Association (WMA) Declaration of Helsinki on ethical principles for medical research involving human subjects. Other relevant texts may need to be identified and consulted during the project's initiation.

3.1 Ethics principles

- **Consent:**

Consent is a fundamental principle under EU law that any intervention in the field of biology and medicine cannot be performed without free and informed consent of the person concerned. Further, consent is also one of the grounds legitimizing the processing of personal data under the General Data Protection Regulation.

However, it must be clear to all parties involved that consent to participation to a trial or a clinical study and consent to the processing of personal data are different:

- 'consent to participation to a trial or a clinical study' is a procedural ethics requirement. Not only is it a good practice highlighted as necessary by many international conferences and declaration, but it is also mandatory under national and European legislation governing clinical trials and studies.
- 'consent to the processing of personal data' is one of the six (6) possible legal grounds provided by the GDPR. Consent to the processing of personal data has several requirements, which are different from those of 'consent for participation to a trial or a clinical study'.

- **Protection of vulnerable persons**

Vulnerable persons are generally associated to children, elderly, or patients. However, vulnerability must be evaluated on an *ad hoc* basis, taking in consideration the context of the research protection and the selection of the research participants. The validity of consent is (among other points) determined by the legal capacity of the person concerned to provide their consent. Minors are a typical category of persons whose consent can be questionable in the absence of consent of their parents or legal guardians. Other examples may include persons with diminished mental faculties and/or incapacitated persons.

- **Ethics committee validation**

Under clinical trial rules, a research protocol must be submitted for consideration, comment, guidance, and approval to the concerned research ethics committee before the study begins. This committee must be transparent in its functioning, must be independent of the researcher, the sponsor and any other undue influence and must be duly qualified. It must take into consideration the laws and regulations of the country or countries in which the research is to be performed as well as applicable international norms and standards.

More generally (including outside the context of clinical trials), a project may decide (or be required) to establish an independent ethics advisory committee, comprising suitably skilled and independent persons who can provide feedback on the project's constraints, objectives, and progression.

The committee must have the right to monitor ongoing studies. The researchers must provide monitoring information to the committee, especially information about any serious adverse events. No amendment to the protocol may be made without consideration and approval by the committee. After the end of the study, the researchers must submit a final report to the committee containing a summary of the study's findings and conclusions.

- **Patients' rights**

It is critical that patient's rights are protected effectively. The patient always has the right of access to preventive health care and the right to benefit from medical treatment under the conditions established by national laws and practices. A high level of human health protection must be ensured in the definition and implementation of all the Union's policies and activities.

- **Transparency**

Patients must receive information in a manner and at a level of detail which is appropriate to ensure that they adequately understand the project's scope, ambitions, and possible impacts. This implies that information must be provided in writing in a sufficiently clear and accessible manner, that key topics are covered, and that a spoken explanation is available to provide further details as required. Furthermore, the information must be continuously available to the patient in a manner that allows them to continue to evaluate and reflect upon their participation, and to express their wishes in this respect (e.g., on the project/ institution website).

- **Risk monitoring**

Any medical research that aims to result in a specific treatment strategy (including personalised treatment recommendations) presents potential risks to the patients, even if no new medical substances or treatments are piloted. For this reason, risk should be monitored and evaluated on a continuous basis.

3.2 Data protection principles

- **Fair and lawful**

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject. Therefore, open, and honest communication with the data subject concerning the processing activities must be in place. Furthermore, personal data may only be collected for specified, explicit and legitimate purposes and may not be further processed in a manner that is incompatible with those purposes.

- **Quality and data storage**

The data collected must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. The personal data processed must be accurate and, where necessary, kept up to date. Therefore, every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, are erased, or rectified without delay. Personal data is stored in identifying format for no longer than is necessary for the purposes of processing.

- **Data security**

This is also a principle of EU data protection law: the GDPR requires that, where a type of processing using new technologies, and considering the nature, scope, context, and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (DPIA).

Data concerning health is considered as inherently privacy sensitive, and any processing activities therefore must be subject to elevated requirements of security and confidentiality, and particular care should be taken in project envisaging to apply a 'big data' analytics approach, implying that information from multiple sources will be brought together and comparatively analysed. Further, the suggesting of personalised treatment options based on this process creates additional safety concerns. Therefore, measures are required that safeguard the data from an information privacy perspective.

To mitigate data protection and privacy harms and to reduce security risks, it is a fundamental principle of EU data protection law that the processing of personal data should always be kept to a minimum. As stated in the GDPR, personal data should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".

3.3 Open access requirements

- **Communication of results**

Scientific research supposes communication of the results through publication. The open access requirement of the EU research programme means that the academic publication relaying the results of a project should be accessible to the public free of charges. Open access to publication requires that the underlying research data be made available as well. Consortium partners have the obligation to make available for access, mining, exploitation, reproduction, and dissemination the research data (as specified in the Data Management Plan) and the associated metadata. Making data available in open access is a processing operation in the meaning of the GDPR. However, personal data are considered as confidential and should not be made accessible to the public as such without restriction, and for an unlimited duration.