“SERICS Ethics and Integrity Review System”

(SERICS Guidelines)

25.07.2024

Abstract

This document has been drafted under the mandate of the SERICS Foundation's Scientific Committee. It supports the SERICS Foundation’s activities and stresses the importance of research integrity and ethical issues, and integrate any other behavioral code on ethical values that have been adopted by Serics partners.

This document has been drafted following “The European Code of Conduct for Research Integrity (revised edition 2023)” and with the principles of “The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research” (respect for persons, beneficence, justice, and respect for law and public interest) and considering as a valuable source of information the Italian CNR guidelines and practices on research integrity.

The primary purpose of this initiative is to define a framework for indicating responsibility and to serve the SERICS research community as a framework for self-regulation.

As for publications, adhesion to the COPE standards is suggested, whereas it is applicable.

The SERICS Guidelines should integrate with the rules and procedures in force by each institution where the researcher belongs.

In any case, the allegation of misconduct that is related to the research activity conducted for the SERICS project should also be channelled through the practices of each institution to which the researcher is primarily affiliated.

All the researchers involved at any level with the research, development and dissemination activities promoted by the SERICS Foundation will comply with the “SERICS Ethics and Integrity Review System Guidelines” (SERICS Guidelines) as a document stating the professional, societal, ethical, and moral responsibilities of the researchers participating in SERICS and of the third parties involved in.

	INDEX	
	Preamble	
	PART A - Integrity of research	
Section 1	*Scope and nature of the Guideline*	
Section 2	*Objectives*	
Section 3	*Principles*	
Section 4	*Standards of good and responsible research*	
Section 5	*Institutional responsibilities*	
Section 6	*Expectations and engagement of researchers*	
Section 7	*Proactive research, safeguards and collaboration*	
Section 8	*Research ethics and governance*	
Section 9	*Gender good practices*	
Section 10	*Research-quality management*	
Section 11	*Intellectual property rights*	
Section 12	*Dissemination and publication of research findings*	
Section 13	*Ethical conduct*	
Section 14	*Final general notes*	
	PART B – Ethics issues	
Section 15	*Introduction*	
1.	*Compliance of SERICS with ethical principles and rules*	
2.	*Ethical issues arising from SERICS*	
3.	*Ethics Assessment*	
Section 16	*Human participants*	
1	*Principles to be applied*	
2	*Informed consent*	
3	*Ethics Assessment Checklist*	
Section 17	*Protection of personal data*	
Section 18	*Requirement on dual use and Misuse of technologies and infrastructures for research activity*	
1	*Protection of security: "Dual use" and misuse of technologies*	
1.1	*Security*	
1.2	*"Dual use" technologies*	
1.3.	*Misuse of technologies*	
2.	*Ethics management*	
3	*Ethics Assessment Checklist*	
Section 19	*Artificial Intelligence*	
1.	*Introduction*	
2	*Principles*	
3	*Requirements to implement the principles*	
4	*Ethics Impact Checklist*	
Section 20	*Other legal and ethical issues*	
1.	*Introduction*	
2	*Rights on the results of the Project*	
2.1.	*IPR Checklist*	
3.	*Open access*	
3.1.	*Introduction*	
3.2.	*Scope of the rules on open data*	
3.3.	*Research data*	
3.4.	*Principles FAIR*	
3.5.	*Data and Research Infrastructures*	
3.6.	*Checklist*	
	Attachments and Annexes	
Annexs *Human Partecipants*		
	Annex A1 *Information Sheet For Participants – Non Anonymous Interviews* *Annex A2* *Information Sheet For Participants General Surveys* *Annex A3* *Information Sheet For Participants – Public Participation* *Annex B1*	

	Consent Form For Participants – Non Anonymous Interviews *Annex B3* *Consent Form For Participants – Public Participation* *Annex C* *Ex-Post Questionnaire*	
Attachments Protection of personal data		
	Attachment 1 *Attachment 2* *Attachment 3* *Attachment 4* *Attachment 5* *Attachment 6* *Attachment 7*	

SERICS Guidelines

Preamble

The SERICS Guidelines (hereinafter referred to as the Guidelines) are intended to highlight the values, principles, and rules of good research practice so that researchers and institutions in SERICS are aware of their responsibility in carrying out research, especially through the infrastructure.

The Guidelines are addressed to the staff involved in SERICS (both academic and non-academic), as well as the collaborators and other third parties collaborating with the project or providing goods and services.

Guidelines concern all aspects of innovation, knowledge, exchange, publications, dissemination and research impact, in order to identify, evaluate and manage any deviations or violations of the principles and values of good research practice.

In fact, the indications provided on the subject of consent and the communication of knowledge have particular importance in these guidelines.
.

The present document is divided into 2 parts:

- Part A refers to the duties of the integrity of research.
- Part B is related to the ethical issues arising from the research activities within the Project.

In addition, enclosed are templates and other documents useful for implementing the rules and recommendations in the Guidelines.

PART A

Section 1

Scope and nature of the Guideline

The present Guidelines range from broad ethical principles to more detailed issues regarding carrying out the research and other activities provided within the Project.

The Guidelines are based on the values, principles, conditions and best practices outlined in the following sources:

- European Science Foundation and ALLEA (All European Academies) 2017. The European Guideline of Conduct for Research Integrity. (http://www.allea.org/wp-content/uploads/2017/03/ALLEA-European-Guideline-ofConduct-for-Research-Integrity-2017-1.pdf);
- EU Charter of Researchers https://euraxess.ec.europa.eu/jobs/charter/european-charter
- EU Charter of Fundamental Rights (Article 13);
- Montreal Statement on Research Integrity in Cross-Boundary Research Collaborations (2013) https://www.wcrif.org/guidance/montreal-statement;
- EU Commission gender equality strategy 2020-2025;
- International Labour Organization (ILO) Convention on combating violance and harassment in the world of work.

Section 2

Objectives

The main objectives of the Guidelines are:

- To underpin the SERICS's commitment to effective research integrity and collaboration;
- To help researchers and other staff members, as well as the Institutions involved in SERICS, to carry out the activities foreseen in the Projects properly;
- To provide public authorities with information to assess the activities put in place within the Project.

Section 3

Principles

The Guidelines reaffirm the research integrity principles such as:

- *Reliability* in ensuring the quality of research reflected in the design, the methodology, the analysis and the use of resources;
- *Honesty* in developing, undertaking, reviewing, reporting and communicating research in a transparent, fair and unbiased way;
- *Respect* for colleagues, research participants, society, ecosystems, cultural

heritage and the environment;

- *Accountability* for the research from idea to publication, for its management and organisation, for training, supervision and mentoring, and its wider impacts.

Section 4

Standards of good and responsible research

The fundamental principles of research integrity are applied in all phases of the SERICS project.

Research activities and their scopes in SERICS are expected to be transparent throughout the research process (execution, reporting, assessment and communication).

SERICS ensures inclusive culture and equal opportunities.

Researchers and institutions must demonstrate moral and intellectual honesty in conducting and reporting research. Responsible conduct refers to information, data reports and publications.

Researchers benefit from independence, avoid conflicts of interest and never use their knowledge to counter the SERICS scopes.

SERICS partners ensure that their views, ambitions and convictions do not compromise the objectives of the SERICS project. Prejudice and conflict of interest do not prevail over the professionalism of the scientific conduct.

In SERICS, the proper management and protection of both research and personal data are ensured.

Adequate records and other supporting documentation are provided to fulfil the obligations arising from the Grant Agreement.

Section 5

Institutional responsibilities

Roles and specific duties to research teams and individual research are assigned with clarity and impartiality, respecting the qualifications and expertise.

SERICS promotes a transparent research environment to support mutual cooperation and the open exchange of ideas and research skills.

Appropriate supervision and direction of researchers and research teams are ensured.

Section 6

Expectations and engagement of researchers

Researchers are expected to adopt and maintain professional standards.

Researchers must be familiar with high scientific and ethical standards and adhere to legal regulations and scientific and ethical guidelines.

All research teams and Work Packages (WPs) of SERICS accept their responsibilities and recognise the best practices in their research field.

Section 7

Proactive research, safeguards and collaboration

SERICS promotes the values and principles of research integrity and ensures research freedom.

SERICS avoid discrimination and risk of coercion.

The risk of misconduct and generally irresponsible practices should be minimised while merit and transparent communication amongst colleagues is pursued.

Researchers must be ready to acknowledge new data, revise their views according to the research findings and adopt new positions based on the availability of new information.

Researchers operate with the respect of/towards all people, including Indigenous people and local communities when involved in research.

Researchers observe regulations and recommended practices such as: obtaining informed consent, equity, safeguarding vulnerable groups, communicating incidental findings, protecting the safety of researchers during research activities.

Collaboration is essential, and working collaboratively is key to addressing certain research issues concerning managing troubles in SERICS.

Tasks are distributed among SERICS Partners according to their specific capacity for hosting, training, and mentoring. All SERICS Partners provide local training through research for the seconded staff and contribute to network-wide training activities, including providing contacts.

Section 8

Research ethics and governance

All research carried out in SERICS must comply with relevant legal, regulatory, professional and ethical requirements.

Researchers unsure whether certain legal requirements apply to their activities should seek advice before performing research.

All permits, approvals and relevant documents must be in place to perform research activities and be updated as plans change.

Section 9

Gender good practices

Research in SERICS takes into account gender equality.

SERICS should aim to balance the representation of men and women.

This Guideline recommends the promotion of equal opportunities between men and women.

Evaluation and recruitment in SERICS activities should respond to principles and practices of gender equality and should be anti-discriminatory based on sex, gender identity and sexual orientation.

Researchers are treated equally regardless of their sex or gender identity at all levels of research activities and processes. This also entails gender balance at all levels of personnel assigned, including at the supervisory and managerial levels.

The use of sexist and gender-discriminatory language is not allowed in the communication of research findings, written reports, oral presentations and publications.

Section 10

Research-quality management

The quality of research is an essential aspect of achieving the SERICS objectives. Researchers should assess the following issues:

- Good research questions to address the SERICS topics;
- Appropriate research methodology for responding to research questions;
- Punctual conduct and reporting of the research;
- Scientific and ethical adequacy of the research;
- Good data management;
- Sufficient and appropriate generation/processing of data, documentation, analysis, use and storage of biological material;
- Timely and public dissemination of research and its outcomes;
- Regular reviews as well as peer review and publications review procedures;
- Integration, implementation and development of practices to strengthen gender equality.

Section 11

Intellectual property rights

All subjects involved in the research activities are requested to respect the Intellectual Property Rights (hereinafter referred to as IPRs) as provided in the relevant legislation and regulation.

Section 12

Dissemination and publication of research findings

Research results are disseminated by disclosing them to the public by appropriate means, including in scientific publications.

Open access to scientific publications shall be ensured under the rules and practices established by the European Union and by other national and international bodies and professional groups.

Section 13

Ethical conduct

When involved in SERICS research activities, the Guidelines invite to avoid unethical conduct, in particular those as follows:

- allowing funders, sponsors, or others to jeopardise independence and impartiality in the research process or unbiased reporting of the results.
- misusing seniority to encourage violations of research integrity or to advance one's own career;
- delaying or inappropriately hampering the work of other researchers;
- misusing statistics, for example, to inappropriately suggest statistical significance;
- hiding the use of AI or automated tools in the creation of content or drafting of publications;
- withholding research data or results without justification;
- chopping up research results with the specific aim of increasing the number of research publications ('salami publications');
- citing selectively or inaccurately;
- expanding unnecessarily the bibliography of a study to please editors, reviewers, or colleagues or to manipulate bibliographic data;
- manipulating authorship or denigrating the role of other researchers in publications;
- re-publishing substantive parts of one's own earlier publications, including translations, without duly acknowledging or citing the original (self-plagiarism);
- establishing, supporting, or deliberately using journals, publishers, events, or services that undermine the quality of research ('predatory' journals or conferences and paper mills);
- participating in cartels of reviewers and authors colluding to review each other's publications;
- misrepresenting research achievements, data, involvement, or interests;
- accusing a researcher of misconduct or other violations in a malicious way;
- ignoring putative breaches of research integrity by others or covering up inappropriate responses to misconduct or other institutional violations.
- discriminating, bully, sexually harass and use aggression or violence against others;
- bribing others by offering goods, services and money;

- having conflicts of interest and refrain from unfounded claims;
- accepting gifts or donations that would signify conflict of interest or exercise unauthorised influence;
- downloading illegal software;
- downloading, distributing and sending racist, offensive, insulting, (sexual) harassing texts, messages, emails and images;
- disclosing or distributing confidential information;
- taking pictures or making (videos) recordings of persons, lectures and presentations without consent or information of the persons involved;
- using others' texts or photos without the permission to use them. This also concerns images found on the internet.

Section 14

Dealing with violations and allegations of misconduct

In case of a breach of the duties of research integrity, the following principles need to be incorporated into any investigation process:

- anyone accused of research misconduct is presumed innocent until proven otherwise;
- investigations are fair, comprehensive, and conducted expediently without compromising accuracy, objectivity, or thoroughness;
- the parties involved in the investigation declare any conflict of interest that may arise during the investigation;
- measures are taken to ensure that investigations are carried through to a conclusion;
- investigations are conducted confidentially in order to protect those involved;
- institutions protect the rights of bona fide whistle-blowers during investigations and ensure that their career prospects are not endangered;
- general procedures for dealing with violations of good research practice are publicly available and accessible to ensure their transparency and uniformity;
- persons accused of research misconduct are given full details of the allegation(s) and are allowed a fair process for responding to allegations and presenting evidence.
- investigations into research misconduct consider the role of both individuals and institutions contributing to the breach of good research practice;
- action is taken against persons for whom an allegation of misconduct is upheld, which is proportionate to the severity of the violation;
- appropriate restorative action is taken when researchers are exonerated of an allegation of misconduct.

Section 15

Final general notes

The present Guidelines reaffirm the obligations provided by the European Union, national or international legal sources, and promote the highest scientific and ethical

conduct, but they are not intended to be exhaustive. They should be considered as guidance to remind all people involved in SERICS on how to engage responsively in ethical principles, behaviours and standards in their everyday working activities for SERICS.

PART B – Ethics issues

Section 15

Introduction

1. Compliance of SERICS with ethical principles and rules

SERICS has to comply with the ethical principles and rules provided by the European Union Law and with the international and national legislations.

The purpose of this Section is thus to provide practical guidance for properly assessing and managing the ethical issues applicable to the project at issue.

When referring to ethical principles and rules in this document, we consider general or specific norms dealing with the possible contrast between the freedom of research and other fundamental interests, such as human rights, security, etc.

Ethical norms are provided by several EU legal texts such as:

– Treaty on European Union (TEU) and Treaty on the functioning of the European Union (TFEU);
– European Charter of Fundamental Rights;
– The Universal Declaration of the Human Rights of the General Assembly of the United Nations;
– The Council of Europe Convention on the Protection of Human Rights and Fundamental Freedoms.
– Specific disciplines have to be applied to specific topics, such as the protection of personal data (see Regulation (EU) 2016/679, General Data Protection Regulation – "GDPR"), the norms concerning security, Artificial Intelligence, and so on.

In addition, the present "Guidelines" have been drawn up taking into consideration the cases law of the Court of Justice, as well as the recommendations, opinions and other documents issued by EU, international and national bodies; and the documents and guidelines adopted by the European Commission, such as "EU Grants: How to complete your ethics self-assessment".

2. Ethical issues arising from SERICS

The ethical issues which may arise from the activities carried out within SERICS will be mainly as follows:

1) Involvement of Human Participants;
2) Protection of Personal Data;
3) Dual use and Misuse of technologies and infrastructures for research activity;
4) Research on and production of Artificial Intelligence;
5) Other ethical and legal issues, i.e. Open Science and Open Data.

The following paragraphs will show the main ethical requirements and the documents to make available for the ethical assessment and the reporting activities regarding each of the above-mentioned issues. The document "EU Grants: How to complete your ethics self-assessment" provides further guidance.

3. Ethics Assessment

For each ethics issue as above mentioned, the Infrastructure, and in particular the Coordinator, is expected to carry out an ethical assessment (EA).

An EA can be part of a regular ethics assessment, which consists of the following phases[1]:

i. carrying out an EA analysis; to do so in the following paragraphs a checklist will be provided[2];

ii. elaborating the documents implementing the measures identified within the checklist analysis, e.g. protocols, policies, template of information sheets, data management plan, risk management assessment; etc.

iii. review and audit the EA by an ethics adviser/ethics committee.

iv. periodic updating of the above-mentioned process (it is recommended to review the EA at least each 12 months or when normative or operational changes may occur).

[1] See as an example of good practice the document "Ethics assessment for research and innovation - Part 2: Ethical impact assessment framework" which is available at https://satoriproject.eu/media/CWA17145-23d2017.pdf
[2] based on the document "EU Grants: How to complete your ethics self-assessment" above mentioned.

Section 16

Human participants

1. Principles to be applied

The involvement of the human participants has to be put in place with the observation of the principles as follows:

a) **Dignity**, i.e. the respect of the essence of the fundamental rights of the persons and their physical integrity;
b) **Self-determination**, i.e. persons will be able to decide freely if they participate or not in the Project's activities;
c) **Proportionality**, i.e. the involvement of the individuals, has to be justified and strictly necessary to the achievement of the objective of the Project;
d) **Precaution**, i.e. the individuals will be involved in the activities, avoiding any additional risk;
e) **Solidarity**, i.e., considering the interests of the persons and protecting them, especially vulnerable people.

In the case of interviews, to comply with the principles mentioned above, the SERICS Partners researchers are requested to put in place the actions as follows:

- All persons interviewed/involved will voluntarily participate in the project, giving their informed consent, responding to the call of interest, or participating in the survey and the events. The participants will be able to withdraw from the Project at their own discretion at any moment without any consequences.
- The persons involved in the interviews (e.g., stakeholders) will be fully informed through the information sheet (see the example of the template enclosed in Attachments), and they will express their consent by signing the informed consent form (see the example of the template enclosed in Attachments).
- Any derogation from the obligation to collect informed consent has to be justified and discussed with the relevant authorities and bodies.

2. Informed consent

Concerning the procedure to collect informed consent, the following directives should be implemented:

A) The persons involved in the project's activities must be informed about the project's subject, its aims, the use of the personal data collected, their storage and protection, and the methods of storage and protection.

In case of interviews or participation in events:

• the person will be previously informed about the research activities and the scientific aim of the interview; he/she will be invited to avoid offensive or discriminatory comments;

• in particular, the person will be informed that her/his interview may be published or disclosed to the public;

• the person will be informed that she/he will have the right to withdraw his/her consent until the publication;

• the person concerned has to give her/his written consent to the interview, and for its processing and publishing.

The information sheet and the informed consent forms should be translated into the mother language of the SERICS participants.

Information is not requested when this will be extremely difficult (e.g. collection of data from social networks or use of data/materials deriving from historical archives). However, in such cases, it is advisable or mandatory (if a legal disposition provides so, see for example Articles 110 and 110 bis Legislative Decree no. 196/2003) to request the authorisation/opinion of the relevant ethical committee or other body.

B) The informed consent template will not be signed, nor personal data of the persons involved will be provided in the following cases:

- in case of general surveys, when data are collected anonymously;
- in case of recording of events or other situations which may affect the security of the persons;
- if the contents of the interview or the situation and the context may expose the person to danger;
- if this is specifically required by the participant;
- In any other case the researchers argue is not opportune or necessary to collect personal data.

In order to avoid any doubt, when the signature of the consent is not required, anyway an adequate information must be provided.

For this reason the following procedures and documents are required

Researchers should provide the following:	**See Annex A information Sheets**
The information sheets for participants	**Non-Anonymous Interviews Annex A1** **General Surveys Annex A2** **Public Participation Annex A3**
Those involved will read and, if agreed, they will sign the template of the informed consent	**See Annex B Informed consent sheets**
Consent Form For Participants	**Non-Anonymous Interviews Annex B1** **Public Participation Annex B3**

The absence of informed consent, as well as the collection of personal data, will be justified by the researcher in the Ex-post Questionnaire (see Annex C). The aim of this questionnaire is to provide evidence that the appropriate measures set for the SERICS consortium were followed and to inform about divergences.

3. Ethics Assessment Checklist

HUMANS	YES/	NO	Information to be provided in the proposal	Description
Does your activity involve human participants?	☐	☐	Please describe the modality of involvement of the individuals and provide information in one of the subcategories below	

If **YES:**	Are they volunteers?	☐	☐	1) Details on recruitment, inclusion and exclusion criteria and informed consent procedures. 2) Details on unexpected findings policy. 3) Approval of ethics committees (if required by law or practice).	
	Are they healthy volunteers for medical studies?	☐	☐	1) Details on recruitment, inclusion and exclusion criteria and informed consent procedures 2) Details on unexpected findings policy. 3) Approval of ethics committees (if required by law or practice).	1) Copies of ethics approvals. 2) Informed consent forms and information sheets.
	Are they patients for medical studies?	☐	☐	1) Details on the typologies of patients 2) Justification on the necessity to involve patients 3) Details on recruitment, inclusion and exclusion criteria and informed consent	

				procedures 4) Details on unexpected findings policy. 5) Approval of ethics committees (if required by law or practice).	
	Are they children/adolescents or potentially vulnerable individuals or groups?	☐	☐	1) Details on the typologies of vulnerable people 2) Justification on the necessity to involve vulnerable people 3) Measures to protect vulnerable people and avoid their exploitation 4) Measures to ensure the respect of self-determination of the vulnerable individuals 5) Details on recruitment, inclusion and exclusion criteria and informed consent procedures 6) Details on unexpected findings policy.	

				7) Approval of ethics committees (if required by law or practice).	

Section 17

Protection of personal data

The activities within SERICS imply the collection of personal data for the purposes of the project, considering that they are proportionate to its general aims.

Personal data will be collected in compliance with the GDPR.

Personal data is defined by the GDPR (see Article 4 (1)) as follows:

‘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’.

1. General principles

In line with the EU legislation, the consortium will respect the following principles (see Article 5 GDPR):

(a) data are collected, processed and stored in a lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

(b) data are collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (‘justification’);

(c) collection is made in an adequate, relevant and limited manner to the extent that is necessary in relation to the purposes for which they are processed (‘data minimisation’);

(d) data are accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

(e) data are 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 (‘storage limitation’);

(f) data are processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

2. Rules for processing personal data

The following rules will be followed to process personal data, as well as for storage, protection, retention and publication of such data:

a) The data will be processed according to the project's aims, taking into account the EU and national legal norms.

b) In any case, to prevent any possible harm to the persons interviewed or in other manner involved, **information concerning identity will not be disclosed outside the research group, and all personal data will be pseudo-anonymised**;
c) After collection, personal data will be **processed pseudo-anonymised** and they will be **electronically encrypted** and be shared for study purposes only in aggregated form within the data management system;
d) Appropriate measures will be taken to prevent unauthorised use of study information and to seek respondents' consent for the uses of data within the Project.

3. Particular cases:

i) Interviews: The transcription or the recording of the interview may be published in a non-anonymous manner if it is useful for the Project, and this might not affect the dignity, human rights and security of the person. For this to be possible, the interviewee will sign the informed consent template in his/her mother language.

ii) ***Surveys***: As mentioned above, participants will not provide their personal details and, therefore, **the templates filled in will not be linked to specific persons**.

The templates (forms with questions) will be gathered by a researcher, who will be specifically appointed by each beneficiary/partner as responsible of the data processing and conservation. The researcher will extract the data from the templates and she/he will store the raw data in a dataset, managed by a person appointed by the Coordinator on the server of the latter.

Other researchers may access the dataset through a password supplied by the Coordinator.

They will process only pseudo-anonymous information showed in general terms without any link to specific persons.

iii) Workshops, fieldtrips, performances: The transcription of the recording and its use in the project's results (for instance, to produce documentaries or publications) will be allowed, subject to compliance with rules concerning informed consent.

iv) Images and Street Photography:

Photograph of an identifiable natural person
Before the exposition and the publication, please follow considerations before reaching a final decision:
a) whether the photo was taken in a public place;
b) whether the individual is a public person;
c) whether the publication was in the public interest; and
d) whether the photograph was taken during a public event.

When the photographer intends to publish or commercially use a photograph identifying a data subject, the provisions of GDPR must be satisfied. This shall mean that no processing shall be allowed without the informed consent of the data subject. Although the GDPR does not specify that consent has to be in writing, a written consent is recommended.

If, due to the restricted circumstances of the shot, the photographer is not in a realistic position to obtain the consent and would still like to use the photograph for purposes falling outside the household exemption, we recommend the blurring of the face as a possible approach to render the individual unidentifiable.
The photographer should seriously consider the need to take pictures of minors. In case of need, the faces of minors should always be blurred or pixelated.
Photos where individuals inadvertently appear in the background
It will not normally be necessary to obtain the specific permission of all who appear incidentally in the background of shots where they are clearly not the focus of the image.

Photos of small crowds/events or groups
Where the image is of a crowd, this is unlikely to be personal data as the individuals will not be identifiable. The GDPR will not therefore apply.

Where an image does not focus on one individual or group of individuals, the data is unlikely to be personal data. Also, it may not be practicable to obtain the consent of every individual. However, it is good practice to ensure that there are clear signs around the venue indicating that photos are being taken.
We would consider it best practice to have written notices in place advising attendees of the timing of the photo being taken, the purpose of taking the photo and the use to which the image will be put. Prior to the image being taken, there should be an announcement informing individuals that the photo is about to be taken to allow attendees to exercise their right not to participate in the initiative.

Special care should be taken in cases where individuals inadvertently appear in the background during events (e.g., demonstrations, prayers, etc.) or in risk situations. In those cases, it is necessary to take any precautions to avoid and minimize as much as possible any risks to the fundamental rights of the individuals. Be careful if there is a reasonable doubt about a possible mishandled use of the photos.

v) Storage

The personal data, as mentioned above, will be stored in a dataset managed by the researchers. The dataset will be built and managed with specific software, in accordance with the requirements of the EU legislation concerning personal data protection.

Once stored in the database, personal data, such as those included in the statements for informed consent (in case of interviews of non-anonymous natural persons), will no longer be accessible for the project's staff.

Researchers will be able to access only to anonymised data to carry out their analysis.

vi) Storage and destruction

The personal data in the dataset will be destroyed as soon as possible and, in any case, by the end of the Project.

vii) Relationships between SERICS Partners

It is advisable to process and transfer between participants only data without elements

of identification with the persons to whom they relate. Therefore, the data should be pseudo-anonymised and deprived of personal identifiers (such as name and surname), with an exception of the structure that has collected the data and that could need personal data for other purposes.

Nevertheless, if two or more SERICS Partners wish to process the same set of personal data, they are requested to enter into a Joint Data Controller Agreement in accordance with Article 26 GDPR.

Considering the processing of personal data, the main areas of concern are shown in the table here below:

Table 1 Personal data management

What to take into account for the personal data management:
The kind of operation performed with data either manually of by automatic means
The use of databases
The procedures and criteria for obtaining informed consent
The purpose of collecting personal research data and safeguard measures
The recipients and data subjects
The data security measures

4. Ethics Assessment Checklist

PROTECTION OF PERSONAL DATA	YES	NO	Information to be provided in the proposal	Description
Does your activity involve processing of personal data?	☐	☐	1) Details on the data 2) Details of the technical and organisational measures to safeguard the rights and freedoms of the participants/data subjects. These may include: - Project specific data protection policy and/or the contact details of the data protection officer (these must be provided to the participants)	

			- The security measures to prevent unauthorised access to personal data - Anonymisation /pseudonymisation techniques. 3) Details of the informed consent procedures with regard to the data processing (if relevant). 4) Explanation as to how all of the processed data is relevant and limited to the purposes of the project ('data minimisation' principle) 5) Justification of why personal data will not be anonymised/ pseudonymised (if relevant). 6) Details of the data transfers (type of data transferred and country to which data are transferred) 7) Justification and measures to implemented in case of transfer of data outside of the European Union, especially for countries which are not interested by and Adequacy Decision of the European	

				Commission.	
If **YES:**	Does it involve the processing of special categories of personal data *(e.g. sexual lifestyle, ethnicity, genetic, biometric and health data, political opinion, religious or philosophical beliefs)*?	☐	☐	1) Justification for the processing of special categories of personal data (if relevant). 2) Justification to why the project objectives cannot be reached by processing anonymised/ pseudonymised data (if applicable). 3) Describe the procedure concerning the Data Impact Assessment (if necessary)	

	Does it involve profiling, systematic monitoring of individuals, or processing of large scale of special categories of data or intrusive methods of data processing *(such as, surveillance, geolocation tracking etc.)*?	☐	☐	1) Details of the methods used for tracking, surveillance or observation of participants. 2) Details of the methods used for profiling. 3) Assessment of the ethics risks related to the data processing operations. 4) Explanation as to how the rights and freedoms of the participants/data subjects will be safeguarded and harm will be prevented. 5) Describe the procedure concerning the Data Impact Assessment (if necessary) 6) Explanation as to how the data subjects will be informed of the existence of the profiling, its possible consequences and how their fundamental rights will be safeguarded.	

Does your activity involve further processing of previously collected personal data *(including use of pre-existing data sets or sources, merging existing data sets)***?**	☐	☐	1) Details of the database used or of the source of the data. 2) Details of the data processing operations. 3) Explanation as to how the rights of the participants/data subjects will be safeguarded. 4) Describe the procedure concerning the Data Impact Assessment (if necessary) 5) Explanation as to how all of the processed data is relevant and limited to the purposes of the project ('data minimisation' principle) 6) Justification of why the data will not be anonymised/ pseudonymised (if relevant).	

Is it planned to export personal data (data transfer) from the EU to non- EU countries? *Specify the type of personal data and countries involved*	☐	☐	1) Details of the types of personal data and countries involved. 2) Explanation as to how the rights and freedoms of the participants/data subjects will be safeguarded 3) Describe the procedure concerning the Data Impact Assessment (if necessary)	
Is it planned to import personal data (data transfer) from non-EU countries into the EU or from a non-EU country to another non-EU country? *Specify the type of personal data and countries involved*	☐	☐	1) Details of the types of personal data and countries involved. 2) Confirmation of compliance with the laws of the country in which the data was collected.	

When to use the attachment related to Section 17 and Section 16

Human participants

When/how to use the Personal Data	When/how to use the Section 16
To understand and comply with the requirement for the legal processing of personal data	To understand that the involvement of participants in research activities must comply with principles and rights (participation, informed consent, respect of privacy)
Informed consent is one of the legal requirement for the lawful processing of personal data	Informed consent is one of the requirements necessary to recruit/involve people joining the research activities
Informed consent is about: informing about the processing, purpose of the processing, the right**s of the data subject**	Informed consent is about: informing on the research activities to be conducted thanks to the individual's involvement, the possibility to withdraw, the use of the data/information arising from the activity (interviews/surveys)
Procedures and criteria for the involvement of stakeholders and the processing of the**ir** personal data within the SERICS consortium	Procedures and criteria for the involvement and recruitment of external individuals/ participants to the research activities
Instructions for the treatment of personal data for re**search activities: to target** the subjects, the activities to be done, the controller/processors, the transfer of personal data	Instructions for the treatment of personal data for interviews, surveys, public participation

Use of personal data for communication and dissemination activities	Use of personal data when joining the project activities
Instructions for the collection and conservation of personal data during/for events (e.g. conferences, **public events,** both online/in presence)	Instructions for the collection and conservation of data whose scope is the involvement of participants for research activities
To provide an overview of the processing of data and the data flow of personal data in SERICS	To provide an overview of the use of personal data in SERICS for interviews, surveys
To inform about the possibility of the transfer of personal data within and outside the consortium	To inform whether data will be made publicly available, kept confidential and use in the project results

How to Use the attachments

In the Personal data	In the Section 16
Attachment 1: General Information on the Treatment of Personal Data for the SERICS Project	Annex A1 Information sheet for participants non-anonymous interviews *This information sheet is delivered jointly with Attachment 1.* GENERAL INFORMATION ON THE TREATMENT OF PERSONAL DATA FOR THE SERICS PROJECT of the Personal Data Policy. Both must be completed and signed accordingly.
Attachment 2: SERICS Table Purpose of Processing: Scientific Research	Annex A2 information sheet for participants general surveys
Attachment 3: SERICS Table Purpose of Processing: Communication and Dissemination	Annex A3 Information sheet for participants- public participation

Attachment 4: Information on the Treatment of Personal Data for Stakeholders	Annex B2 Consent form for participants – non anonymous interviews
Attachment 5: Informed Consent for Stakeholders	Annex B3 Consent form for participants – public participation
Attachment 6: Informed Consent for Speakers Invited to Conventions and Events	Annex C ex-post questionnaire
Attachment 7: Informed Consent of Conventioneers/Persons Attending Events	

Section 18

Requirement on dual use and Misuse of technologies and infrastructures for research activity

1. Protection of security: "Dual use" and misuse of technologies

1.1 Security

Among these fundamental interests, we can identify the meaning of security in Article 6 of the EU Charter of Fundamental Rights and in the Preamble of the EU Treaty (see also European Council, 2010, Internal security strategy for the EU - Towards a European security model).

Article 6 of the EU Charter recognises the "Right to liberty and security", according to which "Everyone has the right to liberty and security of person". On the other hand, the Preamble of the Treaty of the European Union affirms the objective of establishing an area of freedom, security and justice "to facilitate the free movement of persons, while ensuring the safety and security of their peoples".

Furthermore, according to EU documents[3], "EU internal security means protecting people and the values of freedom and democracy", especially "in ensuring a high quality of life in European society, and in protecting our critical infrastructure by preventing and tackling common threats."

The definition of security is related to the free movement of people and citizens. Consequently, to reach the goal of the free circulation of people, the EU has to ensure their safety and to protect them from any risk.

In research activities, threats to security may arise from:

a) The "dual-use" technologies

b) The "misuse" of technologies

1.2 "Dual use" technologies

Dual-use ("DU") items are typically used for civilian purposes but may have military applications or may contribute to the proliferation of weapons of mass destruction.

Within Research projects focused on civil applications, it is necessary to avoid the notion that dual-use technologies may put persons and infrastructures at risk.

The following technologies may be considered as examples of "DU":

- Agents and technologies that could be misused in the weapons context (e.g. pathogens, toxic chemicals, nuclear material, explosives and software robotic systems);

- Information that could be misused for criminal, terrorist or unethical military activities (among others, vulnerability studies and how to increase the harmful consequences of weapons, such as antibiotic resistance studies);

3 European Council, Internal security strategy for the EU - Towards a European security model, 2010.

- Information that could result in the stigmatisation or discrimination of individuals or groups of individuals;
- Surveillance technologies that could be misused for unethical purposes;
- Data mining and profiling technologies that could be misused for unethical purposes.

The legal discipline of DU technologies is provided by Regulation n. 482/2009, concerning the establishment of the EU regime for the control, export, transfer, broking and transit of dual-use items (see Annex 1 herein enclosed).

The Council Regulation (EU) No 1232/2011 amended the existing EU Dual-Use Regulation regarding authorisations. On the other hand, Regulation (EU) 2019/2199 of 17 October 2019 updated the EU Control List of Dual-use items (see Annex 1).

1.3 Misuse of technologies

The term “misuse” indicates research involving agents and/or equipment or creating knowledge that could be directly employed for criminal or terrorist purposes or unethical military activities or when the research itself could result in stigmatisation and or discrimination of individuals or groups.

Examples of misuse of technologies consist in the use of them to violate fundamental interests, such as[4]:

- providing knowledge, materials and technologies that could be channelled into crime or terrorism
- resulting in chemical, biological, radiological or nuclear weapons and the means for their delivery
- involving developing surveillance technologies that could curtail human rights and civil liberties
- involving minority or vulnerable groups or develops social, behavioural or genetic profiling technologies that could be misused to stigmatise, discriminate against, harass or intimidate people.

The main legal sources concerning the misuses are the following:

- Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items (OJ L 134, 29.5.2009, p.1);
- EU Charter of Fundamental Rights;

[4] See EU Grants: Guidance note — Potential misuse of research: V1.1 — 7 January 2020 EUROPEAN COMMISSION Directorate-General for Migration and Home Affairs Directorate-General for Research and Innovation.

- Biological and Toxin Weapons Convention. Available at http://www.unog.ch/80256EE600585943/(httpPages)/04FBBDD6315AC720C1257180004B1B2F?OpenDocument;
- UN Security Council Resolution 1540. Available at http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1540(2004).
- Regulation (EU) No 1232/2011 of the European Parliament and of the Council of 16 November 2011 amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items.
- REGULATIONS Commission - Delegated Regulation (EU) 2019/2199 of 17 October 2019 amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items. Available at https://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/
- Guidance note 1/2016 - FAQs on the controls of 'Information Security' items and implementation of the Cryptography note exemption
- EC Guidance note — Research involving dual-use items
- EC Guidance note — Potential misuse of research
- EC Guidance note — Research with an exclusive focus on civil applications
- Legal texts imposing sanctions (see https://www.sanctionsmap.eu/)

In summary, if the research has the potential for military applications or for malevolent/criminal/terrorist abuse, details on the potential DU or misuse must be provided, together with the indications of measures that will be taken to prevent/address/mitigate military implications.

2. Ethics management

The research and additional project activities will be carried out in order to avoid any security threats by applying the precautionary principle (see Article 191 TFEU).

This will be realised with the following actions:

i) Involvement of international or national authorities (if any);

ii) Training and informing staff and third persons;

iii) Control over dissemination and other activities.

i) Involvement of national authorities

In accordance with the aforementioned Regulation no. 482/2009, the SERICS Partners will request any necessary authorisation for the export of the "DU" technologies to Third Countries (i.e., States that do not form part of the EU).

ii) Training

Staff members will be trained to handle security issues. This is done to identify the relevant issues and comply with the legal and administrative requirements.

iii) Control of dissemination activities

Results generated by the Project will not be available directly to the public, but only to the senior staff members and to the authorities or associations involved in the project, under the condition of the stipulation of a non-disclosure agreement providing the rules concerning the processing, storage and use of such knowledge.

3. Ethics Assessment Checklist

To identify any possible misuse[5], consider the risks associated with the research planned in the project and any unethical or malevolent ways in which the materials, methods, technologies or knowledge involved could be used.

[5] European Commission, EU Grants: Potential misuse of research: V2.0 – 14.09.2021

SECURITY	YES/NO		Information to be provided in the proposal	Description
Does the Project may generate knowledge, materials and technologies that could be used for criminal or terroristic purposes?	☐	☐	1) Details on the material/ knowledge/technologies 2) Typology(ies) of use for criminal or terroristic purpose? 3) Details of the technical and organisational measures to safeguard the rights and freedoms of the individuals and other relevant interests (infrastructures, environment, animals) 4) Elaboration and contents of the risk management assessment	
Does the Project activities may have as result the development of chemical, biological, radiological or nuclear (CBRN) weapons or any method for their delivery?	☐	☐	1) Details on the material 2) Typology(ies) of use for weapons? 3) Details of the technical and organisational measures to safeguard the rights and freedoms of the	

			individuals and other relevant interests (infrastructures, environment, animals) 4) Elaboration and contents of the risk management assessment	
Does the Project provide the development of materials/methods/technologies and knowledge that could harm humans, animals or the environment if they were released, modified or enhanced.	☐	☐	1) Details on the material/ knowledge/technologies 2) Typology(ies) of potential damages? 3) Details of the technical and organisational measures to safeguard the rights and freedoms of the individuals and other relevant interests (infrastructures, environment, animals) 4) Elaboration and contents of the risk management assessment	
Does the project involve developing surveillance technologies that could curtail human rights and civil liberties?	☐	☐	1) Details on the technologies 2) Typology(ies) of potential risk? 3) Details of the technical and organisational measures to safeguard the rights and freedoms of the individuals and other relevant interests (infrastructures,	

			environment, animals) 4) Elaboration and contents of the risk management assessment	
Does the Project's activities may lead to the discrimination or the stigmatisation of minorities or vulnerable groups?	☐	☐	1) Details on the specific activities potentially dangerous 2) Details on minorities and vulnerable groups 3) Typology(ies) of potential risks 4) Details of the technical and organisational measures to safeguard the rights and freedoms of the individuals and groups 5) Elaboration and contents of the risk management assessment	
Could the materials/methods/technologies or knowledge concerned, physically or in any other way, have direct negative impacts on the security of individuals, groups or States?	☐	☐	1) Details on the material/ knowledge/technologies 2) Typology(ies) of negative impacts 3) Details of the technical and organisational measures to safeguard the rights and freedoms of the individuals, group and security of the States 4) Procedure	

			to obtain authorisations by public authorities (if necessary) 5) Elaboration and contents of the risk management assessment	
Could the unauthorised disclosure of the information/materials/methods/technologies or knowledge concerned prejudice the interests of the European Union or of its Member States?	☐	☐	1) Details on information/material/ knowledge/technologies 2) Typology(ies) of negative impacts 3) Details of the technical and organisational measures to safeguard the security of the European Union and of the Member States 4) Procedure to obtain authorisations by public authorities (if necessary) 5) Elaboration and contents of the risk management assessment	
Does the activity involve non-EU countries? **If YES:** **- Do participants from non-EU countries need to have access to EUCI?** **- Do the non-EU countries concerned have a security of information agreement with the EU**	☐	☐	1) Details on third country 2) Details on the involvement of the non-EU participant 3) Details on the agreement on security between EU and non-EU country (if any) 4) Details of the technical and	

			organisational measures to safeguard the security of the European Union and of the Member States 5) Procedure to obtain authorisations by public authorities (if necessary) 6) Elaboration and contents of the risk management assessment	

Section 19

Artificial Intelligence

1. Introduction

According to the Artificial Intelligence Act ("AIA") of the European Union, "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments" (Article 3 (1) AI Act).

In addition to the Artificial Intelligence Act (which is about to be approved by the European Parliament and by the Council), the EU Institutions have approved other documents providing principles and rules relevant to the development and use of AI in research activities and which will be cited in the next paragraphs.

2. Principles

European Commission in a Communication COM(2019) 168[6] has welcomed six principles for AI that have been elaborated in the Guidelines of the High-Level Expert Group. The Commission has used these principles as a base for the AI Act.

Those principles may be described as follows[7]:

1. Respect for Human Agency: human beings must be respected to make their own decisions and carry out their own actions. Respect for human agency encapsulates three more specific principles which define fundamental human rights: autonomy, dignity and freedom.

2. Privacy and Data governance: people have the right to privacy and data protection, and these should be respected at all times;

3. Fairness: people should be given equal rights and opportunities and should not be advantaged or disadvantaged undeservedly;

4. Individual, Social and Environmental Well-being: AI systems should contribute to, and not harm, individual, social and environmental wellbeing;

5. Transparency: the purpose, inputs and operations of AI programs should be knowable and understandable to its stakeholders;

6. Accountability and Oversight: humans should be able to understand, supervise and control the design and operation of AI based systems, and the actors involved in their

[6] See also other institutional documents referring to those principles, such as the European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust", of 19 February 2020, COM(2020) 65 final

[7] See the description made available by the document of the European Commission "Ethics By Design and Ethics of Use Approaches for Artificial Intelligence", Version 1.0, 25 November 2021

development or operation should take responsibility for the way that these applications function and for the resulting consequences.

3. Requirements to implement the principles

In the following paragraphs are listed the requirements to be filed to put in place the ethical principles applicable to AI.
In the use and design of AI in the research activities, the participants are requested to show how the requirements will be actually met:

i) Human Agency: General Ethical Requirements:

- End-users and others affected by the AI system MUST NOT be deprived of abilities to make basic decisions about their own lives or have basic freedoms taken away from them.

- It MUST be ensured that AI applications do not autonomously and without human oversight and possibilities for redress make decisions: about fundamental personal issues (e.g. affecting directly private or professional life, health, well-being or individual rights), that are normally decided by humans by means of free personal choices; or about fundamental economic, social and political issues, that are normally decided by collective deliberations, or similarly significantly affects individuals.

- End-users and others affected by the AI system MUST NOT be in any way subordinated, coerced, deceived, manipulated, objectified or dehumanized.

- Attachment or addiction to the system and its operations MUST not be purposely stimulated. This should not happen through direct operations and actions of the system. It also should be prevented, as much as possible, that systems can be used for these purposes.

AI applications should be designed to give system operators and, as much as possible, end-users the ability to control, direct, and intervene in the system's basic operations.

- End-users and others affected by the AI system MUST receive comprehensible information about the logic involved by the AI, as well as the significance and the envisaged consequences for them.

ii) Privacy and Data Governance: General Ethical Requirements
- The AI systems MUST process personal data legally, fairly and transparently.

- The principles of data minimisation and data protection by design and by default MUST be integrated in the AI data governance models.

- Appropriate technical and organisational measures MUST be set in place to safeguard the rights and freedoms of data subjects (e.g. appointment of data protection officer, anonymization, pseudonymisation, encryption, aggregation). Strong security measures MUST be set in place to prevent data breaches and leakages.

Compliance with the Cybersecurity Act and international security standards may offer a safe pathway for adherence to the ethical principles.

- Data should be acquired, stored and used in a manner which can be audited by humans. All EU funded research must comply with relevant legislation and the highest ethics standards. This means that all SERICS Partners must apply the principles enshrined in the GDPR.

iii) Fairness: General Ethical Requirements

- Avoidance of algorithmic bias: AI systems should be designed to avoid bias in input data, modelling and algorithm design. Algorithmic bias is a specific concern which requires specific mitigation techniques. Research proposals MUST specify the steps which will be taken to ensure data about people is representative of the target population and reflects their diversity or is sufficiently neutral.

- Similarly, research proposals should explicitly document how bias in input data and in the algorithmic design, which could cause certain groups of people to be represented incorrectly or unfairly, will be identified and avoided. This necessitates considering the inferences drawn by the system which have the potential to unfairly exclude or in other ways disadvantage certain groups of people or single individuals.

- Universal accessibility: AI systems (whenever relevant) should be designed to be usable by different types of end-users with different abilities. Research proposals are encouraged to explain how this will be achieved, such as by compliance with relevant accessibility guidelines. To the extent possible, 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,.

- Fair impacts: Possible negative social impacts on certain groups, including impacts other than those resulting from algorithmic bias or lack of universal accessibility, may occur in the short, medium and longer term especially if the AI is diverted from its original purpose. This MUST be mitigated. The AI system MUST ensure that it does not affect the interests of relevant groups in a negative way. Methods to identify and mitigate negative social impacts in the medium and longer term should be well documented in the research proposal.

iv) Well-being: General Ethical Requirements

- AI systems MUST take into account all end-users and stakeholders and must not unduly or unfairly reduce their psychological and emotional well-being.

- AI systems should empower and to advance the interests and well-being of as many individuals as possible

- AI development MUST be mindful of principles of environmental sustainability, both regarding the system itself and the supply chain to which it connects. Whenever relevant, there should be documented efforts to consider the overall environmental

impact of the system and the Sustainable Development Objectives, where needed, steps to mitigate it. In the case of embedded AI this must include the materials used and decommissioning procedures.

- AI systems that can be applied in the area of media, communications, politics, social analytics, behavioural analytics online communities and services MUST be assessed for their potential to negatively impact the quality of communication, social interaction, information, democratic processes, and social relations (for example by supporting uncivil discourse, sustaining or amplifying fake news and deepfakes, segregating people into filter bubbles and echo chambers, creating asymmetric relations of power and dependence, and enabling political manipulation of the electorate). Mitigating actions must be taken to reduce the risk of such harms.

- AI and robotics systems MUST not reduce safety in the workplace. Whenever relevant, the application should demonstrate consideration of possible impact on workplace safety, employee integrity and compliance standards, such as with IEEE P1228 (Standard for Software Safety).

v) Transparency: General Ethical Requirements

- It MUST be made clear to end-users that they are interacting with an AI system (especially for systems that simulate human communication, such as chatbots).

- The purpose, capabilities, limitations, benefits, and risks of the AI system and of the decisions conveyed by it MUST be openly communicated to end-users and other stakeholders, including instructions on how to use the system properly.

- When building an AI solution, one MUST consider what measures will enable the traceability of the AI system during its entire lifecycle, from initial design to post-deployment evaluation and audit or in case its use is contested.

Whenever relevant, the research proposal should offer details about how the system's decisions will be explainable to users. Where possible, this should include the reasons why the system made a particular decision. Explainability is a particularly relevant requirement for systems that make decisions or recommendations or perform actions that can cause significant harm, affect individual rights, or significantly affect individual or collective interests.

- The design and development processes MUST address all the relevant ethical issues, such as the removal of bias from a dataset. The development processes (methods and tools) MUST keep records of all relevant decisions in this context to allow tracing how ethical requirements have been met.

vi) Accountability and Oversight: General Ethical Requirements

- It MUST be documented how possible ethically and socially undesirable effects (e.g. discriminatory outcomes, lack of transparency) of the system will be detected, stopped, and prevented from reoccurring.

- AI systems MUST allow for human oversight and control over the decision cycles and operation, unless compelling reasons can be provided which demonstrate such oversight is not required. Such a justification should explain how humans will be able to understand the decisions made by the system and what mechanisms will exist for humans to override them.

- To a degree matching the type of research being proposed (e.g. basic or precompetitive) and as appropriate, the research proposal should include an evaluation of the possible ethics risks related to the proposed AI system. This should include also the risk assessment procedures and the mitigation measures after deployment.

- Whenever relevant, it should be considered how end-users, data subjects and other third parties will be able to report complaints, ethical concerns, or adverse events and how these will be evaluated, addressed and communicated back to the concerned parties.

- As a general principle, all AI systems should be auditable by independent third parties (e.g. the procedures and tools available under the XAI approach support best practice in this regard). This is not limited to auditing the decisions of the system itself, but covers also the procedures and tools used during the development process. Where relevant, the system should generate human accessible logs of the AI system's internal processes.

4. Ethics Impact Checklist

ARTIFICIAL INTELLIGENCE	YES/NO		Information to be provided	Description
Does this activity involve the development, deployment and/or use of Artificial Intelligence-based systems?	☐	☐	1) Explanation as to how the participants and/or end-users will be informed about: - their interaction with an AI system/technology (if relevant); - the abilities, limitations, risks	

			and benefits of the proposed AI system/technique; - the manner in which decisions are taken and the logic	

			behind them (if relevant). 2) Details on the measures taken to avoid bias in input data and algorithm design; 3) Explanation as to how the respect to fundamental human rights and freedoms (e.g. human autonomy, privacy and data protection) will be ensured; 4) Detailed explanation on the potential ethics risks and the risk mitigation measures. 5) 5) Detailed risk assessment accompanied by a risk mitigation plan (if relevant). 6) Ethics approvals (if relevant).	
Could the AI based system/technique potentially stigmatise or discriminate against people *(e.g. based on sex, race, ethnic or social origin, age, genetic features, disability, sexual orientation, language, religion or belief, membership to a political group, or membership to a national minority)*?	☐	☐	1) Detailed explanation of the measures set in place to avoid potential bias, discrimination and stigmatisation.	

Does the AI system/technique interact, replace or influence human decision-making processes *(e.g. issues affecting human life, health, well-being or human rights, or economic, social or political decisions)*?	☐	☐	1) Detailed explanation on how humans will maintain meaningful control over the most important aspects of the decision-making process; 2) Explanation on how the presence/role of the AI will be made clear and explicit to the affected individuals. 3) 3)Procedures to acquire Information sheets/Template Informed consent (if relevant)	
Does the AI system/technique have the potential to lead to negative social *(e.g. on democracy, media, labour market, freedoms, educational choices, mass surveillance)* and/or environmental impacts either through intended applications or plausible alternative uses?	☐	☐	1) Justification of the need for developing/using this particular technology 2) Assessment of the ethics risks and detailed description of the measures set in place to mitigate the potential negative impacts during the research, development, deployment and post-deployment phase.	
Does this activity involve the use of AI in a weapon system?	☐	☐	1) Justification for the need 2) Detailed explanation on how humans will	

			maintain meaningful control	
Does the AI to be developed/used in the project raise any other ethical issues not covered by the questions above *(e.g., subliminal, covert or deceptive AI, AI that is used to stimulate addictive behaviours, life- like humanoid robots, etc.)*?	☐	☐	1) Detailed explanation on how the potential ethics issues will be addressed 2) the measures set in place to mitigate ethics risks. 3) Detailed risk assessment accompanied by a risk mitigation plan.	

Section 20

Other legal and ethical issues

1. Introduction

In addition to the ethics issues discussed above, the activities carried out within the Project may pose other juridical and ethical issues.

The next paragraphs of the present Section consider some of these issues, in particular the rights to the results and the need to ensure open access to the data.

In any case, other questions may derive from the implementation of the Project and of the infrastructure. Therefore, a continuous analysis of the ethics and legal aspects should be carried out with the help of the bodies described in the paragraphs above.

2. Rights on the results of the Project.

According to documents of the Commission concerning the management of research projects (i.e. Commission Recommendation C(2008) 1329 of 10.4.2008 on the management of intellectual property in knowledge transfer activities and the Guideline of Practice for universities and other public research institutions attached to this recommendation)

“An effort should be made to better convert knowledge into socioeconomic benefits. Therefore, public research organisations need to disseminate and to more effectively exploit publicly funded research results with a view to translating them into new products and services. Means to realise this include in particular academia-industry collaborations — collaborative or contract research conducted or funded jointly with the private sector — licensing and the creation of spin-offs” (“recital” 2 of the Recommendation).

Public research organisations are requested to effectively exploit publicly funded research results with a proper management system of intellectual property (i.e. knowledge in the broadest sense, encompassing e.g. inventions, software, databases, whether or not they are protected by legal instruments such as patents) (“recital” 3 of the Recommendation).

According to the Commission, “The active engagement of public research organisations in intellectual property management and knowledge transfer is essential for generating socioeconomic benefits, and for attracting students, scientists and further research funding” (“recital” 4 of the Recommendation).

To help the management of intellectual property management and knowledge transfer, the Guidelines provide a “Checklist” in order to improve the way public research organisations manage intellectual property and knowledge transfer.

2.1 IPR Checklist

Principles	**Description of the actions to be implemented**

Principles for an internal intellectual property policy	
1. Develop an IP policy as part of the long-term strategy and mission of the public research organisation, and publicise it internally and externally, while establishing a single responsible contact point.	
2. That policy should provide clear rules for staff and students regarding in particular the disclosure of new ideas with potential commercial interest, the ownership of research results, record keeping, the management of conflicts of interest and engagement with third parties.	
3. Promote the identification, exploitation and, where appropriate, protection of intellectual property, in line with the strategy and mission of the public research organisation and with a view to maximising socioeconomic benefits. To this end, different strategies may be adopted — possibly differentiated in the respective scientific/technical areas — for instance the 'public domain' approach or the 'open innovation' approach.	
4. Provide appropriate incentives to ensure that all relevant staff play an active role in the implementation of the IP policy. Such incentives should not only be of a financial nature but should also promote career progression, by considering intellectual property and knowledge transfer aspects in appraisal procedures, in addition to academic criteria.	
5. Consider the creation of coherent portfolios of intellectual property by the public research organisation — e.g. in specific technological areas	

— and, where appropriate, the setting-up of patent/IP pools including intellectual property of other public research organisations. This could ease exploitation, through critical mass and reduced transaction costs for third parties.	
6. Raise awareness and basic skills regarding intellectual property and knowledge transfer through training actions for students as well as research staff, and ensure that the staff responsible for the management of IP/KT have the required skills and receive adequate training.	
7. Develop and publicise a publication/dissemination policy promoting the broad dissemination of research and development results (e.g. through open access publication), while accepting possible delay where the protection of intellectual property is envisaged, although this should be kept to a minimum.	
Principles for a knowledge transfer policy	
8. In order to promote the use of publicly funded research results and maximise their socioeconomic impact, consider all types of possible exploitation mechanisms (such as licensing or spin-off creation) and all possible exploitation partners (such as spin-offs or existing companies, other public research organisations, investors, or innovation support services or agencies), and select the most appropriate ones.	
9. While proactive IP/KT policy may generate additional revenues for the public research organisation,	

this should not be considered the prime objective.	
10. Ensure that the public research organisation has access to or possesses professional knowledge transfer services including legal, financial, commercial as well as intellectual property protection and enforcement advisors, in addition to staff with technical background.	
11. Develop and publicise a licensing policy, in order to harmonise practices within the public research organisation and ensure fairness in all deals. In particular, transfers of ownership of intellectual property owned by the public research organisation and the granting of exclusive licences should be carefully assessed, especially with respect to non-European third parties. Licences for exploitation purposes should involve adequate compensation, financial or otherwise.	
12. Develop and publicise a policy for the creation of spin-offs, allowing and encouraging the public research organisation's staff to engage in the creation of spin-offs where appropriate, and clarifying long-term relations between spin-offs and the public research organisation.	
13. Establish clear principles regarding the sharing of financial returns from knowledge transfer revenues between the public research organisation, the department and the inventors.	
14. Monitor intellectual property protection and knowledge transfer activities and related achievements, and publicise these regularly. The research results of	

the public research organisation, any related expertise and intellectual property rights should be made more visible to the private sector, in order to promote their exploitation.	
Principles regarding collaborative and contract research:	
15. The rules governing collaborative and contract research activities should be compatible with the mission of each party. They should take into account the level of private funding and be in accordance with the objectives of the research activities, in particular to maximise the commercial and socioeconomic impact of the research, to support the public research organisation's objective to attract private research funding, to maintain an intellectual property position that allows further academic and collaborative research, and avoid impeding the dissemination of the R&D results.	
16. IP-related issues should be clarified at management level and as early as possible in the research project, ideally before it starts. IP-related issues include allocation of the ownership of intellectual property which is generated in the framework of the project (hereinafter foreground), identification of the intellectual property which is possessed by the parties before starting the project (hereinafter background) and which is necessary for project execution or exploitation purposes, access rights (3) to foreground and background for these purposes, and the sharing of revenues.	
17. In a collaborative research project, ownership of the foreground should stay with the party that has	

generated it, but can be allocated to the different parties on the basis of a contractual agreement concluded in advance, adequately reflecting the parties' respective interests, tasks and financial or other contributions to the project. In the case of contract research the foreground generated by the public research organisation is owned by the private sector party. The ownership of background should not be affected by the project.	
18. Access rights should be clarified by the parties as early as possible in the research project, ideally before it starts. Where necessary for the purpose of conducting the research project, or for the exploitation of foreground of a party, access rights to other parties' foreground and background should be available, under conditions which should adequately reflect the parties' respective interests, tasks, and financial and other contributions to the project.	

3. Open access

3.1 Introduction

Open Data Directive (Directive 2019/1024) has updated European legislation on open data and the re-use of public sector information.

The Directive sets the guiding rules for the Member States, which then have to be implemented at the national level with domestic laws. As of today, in Italy, the discipline on Open Data is to be found in the new version of Legislative Decree No. 36/2006, which has been updated to incorporate the provisions of the Open Data Directive.

The Agenzia per l'Italia Digitale ("AgID") has published specific Guidelines to clarify the technical rules to be implemented in order to comply with the new discipline[8].

Furthermore, the European Commission adopted the Implementing Regulation 2023/138 for certain categories of data defined as "high-value". AgID then published another operational guide dedicated to high-value data sets, which specifies that this expression refers to data whose use can be associated with 'important benefits for society, the environment and the economy, in view of their suitability for the creation of

[8] https://www.agid.gov.it/sites/default/files/repository_files/lg-open-data_v.1.0_1.pdf

services, value-added applications and new jobs, as well as the number of potential SERICS Partners of value-added services and applications based on these data sets'.

3.2 Scope of the rules on open data

The rules on the openness of data are binding for public administrations, for public law bodies (including research bodies, such as the CNR), but also for certain types of public and private enterprises, including for instance companies that manage transport or other public services (as laid down in Article 1, paragraphs 2-ter and 2-quater of Legislative Decree 36/2006).

Specifically, these rules concern the re-use of documents containing public data that these enterprises manage. The legislation on open data does not apply to all controlled documents managed by these entities, but there are major exceptions that concern, for instance: documents protected by intellectual and industrial property rights, personal data, documents held for purposes outside the institutional tasks of the public administration or public law body (for the complete list see Article 3 of Legislative Decree 36/2006).

3.3 Research data

Specific provisions concerning research data are contained in the Open Data Directive and Legislative Decree 36/2006.

Article 10 of the directive requires member states to adopt policies to make publicly funded research data openly available. The principle enshrined in the directive is openness by default, i.e. in compliance with the FAIR principles - an acronym that stands for Findable, Accessible, Interoperable and Reusable -, - thus at the same time safeguarding intellectual property rights, personal data protection and confidentiality, security and legitimate commercial interests, according to the principle as open as possible, as closed as necessary.

This provision has been incorporated into Legislative Decree 36/2006 in Article 9-bis.

By 'research data' is meant 'documents in digital format, other than scientific publications, collected or produced in the course of scientific research and used as evidence in the research process, or commonly accepted in the research community as being necessary to validate the conclusions and results of the research' (Article 2 no. 9 of the Directive and Art. 2 co. 1 lett. c-septies of Legislative Decree 36/2006); therefore, it is important to emphasise that scientific publications are not included.

Moreover, the exceptions concerning protecting personal data, intellectual and industrial property and commercial interests remain applicable.

It is also important to emphasise that the research data to which the obligation is that they are made available for commercial and non-commercial purposes are the results of research activities financed with public funds and made public by researchers, organisations carrying out research activities, and/or financing research, through a database managed at the institutional level or on a thematic basis.

3.4. Principles FAIR

The AgID Guidelines define both the technical requirements for implementing the open data legislation and (non-mandatory) recommendations concerning aspects that are important for the open data process but not regulated by law.
Both the common and specific requirements for research data apply to research data. In particular, it is necessary to comply with the principle FAIR (Findable, Accessible, Interoperable, Reusable).
The AgID Guidelines recommend the following requirements to implement those principles[9]:

Findable—The first requirement to ensure data reuse is that the data be findable by machines and humans.

To do this, metadata should be made available through an online searchable resource and a persistent identifier should be assigned to data and metadata.

Various metadata profiles are available; for research data reference is also made to the OpenAIRE project (www.openaire.eu) and its related infrastructure.

For the purposes of these Guidelines, research data MUST also be documented in the national portal dati.gov.it.

Accessible - It must be possible for humans and machines to access data through standard and open protocols.

To make data accessible IT IS REQUIRED:

-allow access to data and metadata from the assigned unique and persistent identifier;

-use standardised and open protocols (e.g. https);

-make metadata always available even when the data is not accessible (either because authentication and access authorisation mechanisms are applied or because it is no longer available).

Interoperable - Data and metadata must be able to be combined with other data and/or tools. For this, they must conform to recognised formats and standards

In order to make data interoperable IT IS REQUIRED:

-to provide data in open format according to the requirements defined in these Guidelines;

-to use relevant standards for metadata;

-to use controlled vocabularies, keywords, thesauri and ontologies where possible;

-to include qualified references to other data or metadata

[9] See the document "How to make your data FAIR", at https://www.openaire.eu/how-to-make-your-data-fair. See the checklist "How fair are your data?" by Sarah Jones and Marjan Grootveld (see https://zenodo.org/record/5111307#.YhEfAd_SKCQ)

Reusable: Data must be well documented so that it can be correctly interpreted, replicated and/or combined in different contexts. Data must also be given a clear and accessible licence so that it can be understood what kind of re-use is allowed. This is without prejudice to the due respect of the limits to re-use arising from European and national data protection legislation.

To make data reusable, it is REQUIRED to:

-make available accurate and well-described data with many relevant attributes;

-assign a clear and accessible licence to use the data;

-make clear how, why, when and by whom the data have been created and processed;

-follow relevant domain standards for data and metadata.

3.5. Data and Research Infrastructures

In the case of the “research infrastructures” in addition to the common requirements, several specifications are added in the case of IRs, among which it is worth mentioning
- the provision of detailed metadata and persistent identifiers (e.g. DOIs), which are available even when the data have restricted access or are not available at all.
- the use of standardised and open protocols (e.g. https) to make accesses
- the standard use of metadata, if possible domain, and controlled vocabularies, keywords, thesauri and ontologies;
- Making it clear how, why, when and by whom the data were created and processed
- Releasing the data under a CC-BY 4.0 or CC-0 licence (thus avoiding proprietary licences) and allowing reuse for derivative works, even for commercial purposes.
- The provision of data via APIs that comply with the "Guidelines on Technical Interoperability of Public Administrations" and the "Guidelines on Technologies and Standards for the Security of Interoperability via APIs of Information Systems", adopted by AgID Determination no. 547/2021.
- The rules for data re-use, as well as the fees and details on how they are calculated, must be published on the websites of the relevant public institutions, public bodies and public enterprises

3.6 Checklist

Principle/Requirements	**Description of the activities to be carried out**
Findable ☐ A persistent identifier is assigned to your data ☐ There are rich metadata, describing your data ☐ The metadata are online in a searchable resource e.g.	

a catalogue or data repository - The metadata record specifies the persistent identifier	
Accessible - Following the persistent ID will take you to the data or associated metadata - The protocol by which data can be retrieved follows recognised standards e.g. http - The access procedure includes authentication and authorisation steps, if necessary - Metadata are accessible, wherever possible, even if the data aren't	
Interoperable - Data is provided in commonly understood and preferably open formats - The metadata provided follows relevant standards - Controlled vocabularies, keywords, thesauri or ontologies are used where possible - Qualified references and links are provided to other related data	
Reusable - The data are accurate and well described with many relevant attributes - The data have a clear and accessible data usage license - It is clear how, why and by whom the data have been created and processed	

☐ The data and metadata meet relevant domain standards	

Attachments and Annexes

Annex A1

INFORMATION SHEET FOR PARTICIPANTS – NON ANONYMOUS INTERVIEWS

You will be given a copy of this information sheet.

This information sheet is delivered jointly with Attachment 1. **GENERAL INFORMATION ON THE TREATMENT OF PERSONAL DATA FOR THE SERICS PROJECT of the Personal Data Policy. Both must be completed and signed accordingly.**

Invitation Paragraph

I would like to invite you to participate in the research project SERICS… [*complete with information about the project within SERICS*]

You should only participate if you want to; choosing not to participate will not disadvantage you in any way. Before you decide whether to participate or not, it is important for you to understand why the research is being done and what your participation would involve. Please take time to read the following information carefully. Ask me if anything is unclear or if you would like more information.

What is the purpose of this project ?

[*complete with information about the project within SERICS*]

Why have I been invited to take part ?

We are inviting different participants to be interviewed coming from a whole range of players [---to be completed with the active role of the targeted partcipant---]

Do I have to take part?

Participation is voluntary. You do not have to take part. You should read this information sheet and if you have any questions you should ask me.

What will happen to me if I take part?

If you decide to take part, you will be given a copy of this information sheet and you will be asked to sign a consent form. I will then discuss the interview procedure with you and arrange to interview you in a private place (for confidentiality reasons) in the premises where you work (or-in a suitable venue in a public local site if you prefer).

The interview will take approximately [---to be completed with the precise duration of the interview---] and be based on an interview guide, but it is designed to be flexible so as to meet your needs. The interview will be recorded if you give the consent to do so. All recordings of data on audio-equipment will be deleted after transcription. Even if you have decided to take part, you are still free to stop your participation at any time during the interview and to have the withdrawal of research data/information related to you.

What are the possible benefits and risks in taking part?

The information I get from the study will help to [---to be completed with the precise specific aims---]

There are no foreseeable risks in participating in the study.

Will my taking part be kept confidential ?

The content of the interview is regarded as strictly confidential and will be held securely until the research is finished. All data for analysis will be anonymised. In reporting on the research findings, I will not reveal the names of any participants or the organization where you work. At all times there will be no possibility for you as individuals to be linked with the data. Personal data will be electronically encrypted and be shared for study purpose only in aggregated form within the management system. The dataset is managed by the Coordinator.

Will the data be publicly available?

The data used will be publicly available only anonymously. Therefore they will not allow the identification of the persons, if such persons do not give the explicit consent to publish personal data.

Publication (including publication on the internet) will not lead (either directly or indirectly) to a breach of the agreed confidentiality and anonymity.

How is this project being funded?

[*complete with information about the project within SERICS*]

What will happen to the results of the study?

They will be used to [---to be completed---] (For example, elaborate publications, reports, documentaries)

Who should I contact for further information?

If you have any questions or you need more information about this study, please

contact me using the following contact details:

[---to be completed with the full contact details and indication of the SERICS partner---].

Thank you for reading this information sheet and for considering taking part in this research.

Annex A2

INFORMATION SHEET FOR PARTICIPANTS - GENERAL SURVEYS

You will be given a copy of this information sheet.

Invitation Paragraph

I would like to invite you to participate in the research project SERICS [*complete with information about the project within SERICS*]

You should only participate if you want to; choosing not to take part will not disadvantage you in anyway. Before you decide whether you want to take part, it is important for you to understand why the research is being done and what your participation will involve. Please take time to read the following information carefully. Ask me if there is anything that is not clear or if you would like more information.

What is the purpose of this project?

[*complete with information about the project within SERICS*]

I am specifically interested in [---to be completed---]

Why have I been invited to take part?

I am doing a general survey through interviews of people concerned by the topics of the project, such as their experiences concerning [---to be completed with the targed experience---] The persons to be interviewed will be involved during this event [---to be completed with the precise indication of the event, e.g., Conferences, seminars, workshops---]

Do I have to take part?

Participation is voluntary. You do not have to take part. You should read this information sheet, and if you have any questions, you should ask me.

What will happen to me if I take part?

If you decide to take part you will be given this information sheet to keep and I will then give you a form with questions to answer.

Even if you have decided to take part, you are still free to stop your participation at any time while filling the form.

What are the possible benefits and risks of taking part?

The information I get from the study will help to [---to be completed with the precise specific aims---]. There are no foreseeable risks in participating in the study.

Will my participation be kept confidential?

This survey is anonymous. You will not provide your personal details, and therefore the form filled in will not be linked to you.

The data will be shared for study purpose within the management system. The dataset is managed by the responsible partner for the SERICS project.

Will the data be publicly available?

The data used will be publicly available only anonymously. Therefore they will not allow the identification of the persons, if such persons does not give his/her explicit consent to publish personal data.

Publication (including publication on the internet) will not lead (either directly or indirectly) to a breach of the agreed confidentiality and anonymity since your personal data will not be made public.

How is this project being funded?

[*complete with information about the project within SERICS*]

What will happen to the results of the study?

They will be used to [---to be completed--- for e.g. elaborate publications, reports, documentaries]

Who should I contact for further information?

If you have any questions or require more information about this study, please contact me using the following contact details: [---to be completed with the full contact details and indication of the SERICS partner---].

Thank you for reading this information sheet and for considering taking part in this research.

Annex A3

INFORMATION SHEET FOR PARTICIPANTS – PUBLIC PARTICIPATION

You will be given a copy of this information sheet.

Invitation Paragraph

I would like to invite you to participate in the research project SERICS

[*complete with information about the project within SERICS*]

You should only participate if you want to; choosing not to take part will not disadvantage you in anyway. Before you decide whether you want to take part, it is important for you to understand why the research is being done and what your participation will involve. Please take time to read the following information carefully. Ask me if there is anything that is not clear or if you would like more information.

What is the purpose of this project?

[*complete with information about the project within SERICS*]

I am specifically interested in [---to be completed---]

Why have I been invited to take part?

I am organising a public participation [---to be completed---]

Do I have to take part?

Participation is voluntary. You do not have to take part. You should read this information sheet and if you have any questions you should ask me.

What will happen to me if I take part?

You have been invited to take part through a call of interest. If you decide to take part you will be given this information sheet to keep and you will be asked to sign a consent form.

Even if you have decided to take part, you are still free to stop your participation at any time during the public event.

The public participation will consist in [---to be completed---]

What are the possible benefits and risks in taking part?

The information I get from the study will help to [---to be completed---]

There are no foreseeable risks in participating in the study.

Will my taking part be kept confidential?

This participation may lead to audio and video material collection to make possible a shared work between the researchers/staff involved in the project. You will be asked a written consent mentioned in the consent form to be signed.

The data will be shared for study purpose within the management system. The dataset is managed by the Coordinator.

Will the data be publicly available?

The data used will be publicly available only anonymously. Therefore they will not allow the identification of the persons, if such persons does not give his/her explicit to publish personal data.

Publication (including publication on the internet) will not lead (either directly or indirectly) to a breach of the agreed confidentiality and anonymity.

How is this project being funded?

What will happen to the results of the study?

They will be used to elaborate [---to be completed--- e.g., publications, reports, documentaries]

Who should I contact for further information?

If you have any questions or require more information about this study, please contact me using the following contact details: [---to be completed with the full contact details and indication of the SERICS partner---].

Thank you for reading this information sheet and for considering taking part in this research.

ANNEX B1

CONSENT FORM FOR PARTICIPANTS – NON ANONYMOUS INTERVIEWS

Project: SERICS

Name of Staff Member [---to be completed---]

Name of Participant [---to be completed---]

1. I consent to participate in the SERICS research project conducted by [---to be completed---Name of the Staff Member] from [---to be completed---Name of the sending organization/institutions/partners]

2. I have been explained the details of the project and I have read and understood the information sheet dated [---to be completed--- dd/mm/yyyy Insert date and version number]. I have had the opportunity to consider the information and asked questions that have been answered satisfactorily. I have been provided with a written information sheet.

3. I understand that the SERICS is designed to gather information for the following research object [---to be completed---]

4. My participation in this project is voluntary. I understand that I will not be paid for my participation. I may withdraw and discontinue participation at any time without penalty, at my own discretion, without any consequences, until [---to be completed--- date dd/mm/yyyy]

5. If I feel uncomfortable in any way during the interview session, I have the right to decline to answer any question or to end my interview.

6. I understand that while information gained during the study may be published, I will not be identified and my personal results will remain confidential.

7. I understand that filmed interviews and audio recording may be needed. I consent to my interview being audio/video recorded.

8. I understand that the staff member will not identify me by name in any reports using information obtained from this interview, and that my confidentiality as a participant in this study will remain secure.

9. I understand that the personal data will be processed in an anonymous manner and that they will be electronically encrypted; that they will be shared for study purpose only in aggregated form within the data management system.

10. I understand that the data will be stored in a dataset managed by the

Coordinator. The dataset will be built and managed with specific software, observing the requirements of the EU legislation concerning the protection of the personal data. The personal data existing in the dataset will be destroyed as soon as possible, and, in any case, by the end of the project.

11. I have been given a copy of this consent form.

Name of the participant [---to be completed---]

Date [---to be completed--- dd/mm/yyyy]

Signature [---to be completed---]

Name of Staff member [---to be completed---]

Date [---to be completed--- dd/mm/yyyy]

Signature [---to be completed--]

For further information, please contact [---to be completed---]

Staff member: [---to be completed--- preferred contact details*]*

Annex B3

CONSENT FORM FOR PARTICIPANTS – PUBLIC PARTICIPATION

Project: SERICS

Name of Staff Member: [---to be completed---]

Name of Participant: [---to be completed---]

1. I consent to participate in the SERICS research project conducted by [---to be completed---Name of the Staff Member] from [---to be completed---Name of the organization/institutions/partners].

2. I have been explained the details of the project and I have read and understood the information sheet dated [---to be completed---Insert date dd/mm/yyyy and version number]. I have had the opportunity to consider the information and asked questions which have been answered satisfactorily. I have been provided with a written information sheet.

3. I understand that the project is designed to gather information for the following research object: [---to be completed---]

4. My participation in this project is voluntary. I understand that I will not be paid for my participation. I may withdraw and discontinue participation at any time without penalty, at my own discretion, without any consequences until [---to be completed--- date dd/mm/yyyy]

5. If I feel uncomfortable in any way during participating in this public/shared event, I have the right to end my participation.

6. Anonymity is optional in this case. Please select from the following 2 options:

    - I agree to be fully identified: YES / NO
    - I wish to remain anonymous: YES/NO

7. I understand that this event may lead to audio and video material collection. I consent to be audio/video recorded during the event.

8. If I wish to remain anonymous, I understand that my confidentiality as a participant in this study will remain secure.

9. I understand that the data will be shared for study purpose only in aggregated form within the data management system.

10. I understand that the data will be stored in a dataset managed by the Coordinator. The dataset will be built and managed with specific software, observing the requirements of the EU legislation concerning the protection of the personal data. The personal data existing in the dataset will be destroyed as soon as possible, and, in any case, by the end of the project.

11. I have been given a copy of this consent form.

Name of the participant [---to be completed---]

Date [---to be completed--- dd/mm/yyyy]

Signature [---to be completed---]

Name of Staff member [---to be completed---]

Date [---to be completed--- dd/mm/yyyy]

Signature [---to be completed--]

For further information, please contact [---to be completed---]

Staff member: [---to be completed--- preferred contact details*]*

ANNEX C

EX-POST QUESTIONNAIRE

Dear Member

In order to meet the ethics requirements of the SERICS Project, please answer the following questions:

1. General characteristics

1.1. How did you finalise the involvement of research participants in the activities of your WP/Task?

Please provide your answer here

1.2. What were the methodology and tools employed in your work (e.g. video or voice recording, interviews, transcription of dialogues, use of social media, personal observation or analysis) Please describe

Please provide your answer here

1.3. Were the objectives of your activities achieved? Was there any change of intention or deviation from the original scopes? If so, please justify the reasons

Please provide your answer here

2. Collaborations

2.1. Did anyone from the SERICS collaborate with you?

Please provide your answer here

3. Unexpected risks/problems

3.1. Did you experience any unexpected problems while preparing/during your fieldwork? Did they have any ethical implications?

Please provide your answer here

3.2. Did you encounter any of the following problems:

- Adhering to social norms or uses
- Recruitment of participants
- Partner institution volunteering to collaborate with you
- Need to ensure confidentiality
- Other risks (Please describe)

3.3. If answered to the previous question, how did you overcome problems?

Please provide your answer here

4. Data collection and data processing

4.1. What kind of personal data did you collect?

Please provide your answer here

4.2. Who accessed these data?

Please provide your answer here

4.3. Did you collect or process any other sensitive information (analysis of political/social conditions, personal opinions) in the course of activities

Please provide your answer here

4.4. Did you provide the participants to the research with the information sheets and collect the informed consent forms duly filled in and signed? If the answer is no, please justify.

Please provide your answer here

4.5. How did you store the other information obtained form participants?

Please provide your answer here

4.6. If applicable, how did you store and aggregate data and information gathered or generated by you (e.g. through analysis, interpretation, conclusions)?

Please provide your answer here

5. Participants

5.1. Did your activities involve vulnerable individuals/groups or disadvantages minorities? Please also explain the way you approach to them and the information obtained

Please provide your answer here

5.2. Did you make all participants able to give their consent and sign the informed consent sheet?

Please provide your answer here

5.3. Did you make the participants aware of the rationale and aims of the SERICS project and the consequences of their participation? (e.g. explaining terms, using a plain language)

Please provide your answer here

5.4. Are participants in your research/work anonymous? Do you think they should be anonymized?

Please provide your answer here

5.5. Was there gender balance in engaging participants to research? (e.g. in the composition of the team for the fieldwork activities, in the participants, in the general public)

Please provide your answer here

6. Miscellanea

6.1 Did you comply with confidentiality rules? What did you do about it?

Please provide your answer here

6.2. Did you use the data or information gathered for deliverables or publications?

Please provide your answer here

Attachment 1

GENERAL INFORMATION ON THE TREATMENT OF PERSONAL DATA FOR THE SERICS PROJECT

Information

The use of your personal data is in compliance with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) hereafter referred to as GDPR[10].

According to the GDPR provisions on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, this information sheet is meant to inform you about the way your personal data are processed by [---to be completed---] in compliance with the above-mentioned regulation and the duty of secrecy/obligation of confidentiality you are bound to.

Contacts

The Data Controller [---to be completed---]

office in [---to be completed---]

contact e-mail: [---to be completed---]

The person responsible for the protection of [partner name] data is [---to be completed---]

contact e-mail: [---to be completed---]

Aims and compulsory elements of the processing

[---to be completed---] processes personal data for the aims provided by the GDPR (i.e. for the implementation of its own institutional tasks and public interests), including the aims of transparency, communication, scientific divulgation and filing.

Processing and preservation procedures

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), *OJ L 119, 4.5.2016, p. 1–88*

Pursuant to Article 5 of the GDPR[11], the personal data will be handled by [---to be completed---] in accordance with the principles of lawfulness, fairness, transparency and minimisation. The data will be conserved for the time necessary for the achievement of the aims for which they have been collected and processed.

In accordance with Article 32 of the GDPR[12], the personal data will be processed on the operative premises of [---to be completed---] using prevalent computer-related and telematics equipment. In compliance with Article 29 of the GDPR[13], the personal data will be processed with the help of expressly designated persons.

The ambit of communication and diffusion

[---to be completed---] will never spread nor subject the personal data to communication without your explicit consent, except for necessary communications that may involve the transfer of data to public authorities, advisers, legal counsels, collaborators or any other subject in order to fulfil legal obligations.

Transfer of personal data

[---to be completed---] may transfer personal data within Member States of the European Union but not within countries that do not belong to the European Union, unless explicit communication to that effect is provided.

[11] GDPR, Art. 5, Principles relating to processing of personal data: 1. Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'); (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); (e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject('storage limitation');(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

[12] GDPR, Art.32, Security of processing: 1. Taking into account 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 controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:(a) the pseudonymisation and encryption of personal data; b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. 3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article. 4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

[13] GDPR, ART. 29: Processing under the authority of the controller or processor: The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

The right to withdraw consent

The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect: (a) the lawfulness of processing based on consent before its withdrawal or (b) further cases of processing of the same data founded on other legal bases (e.g. contractual or legal obligations to which the Data Controller is subject).

Rights of the person concerned

At any moment, it is possible to access, rectify, cancel or object to your personal data, as such may pertain to its use or collection. This is provided in conformity with Articles 15-22 of the GDPR, which provide the following rights:

a) To require the confirmation on the existence or non-existence of your personal data[14];
b) To obtain indications of the processing purposes, the personal data category, the recipients and the storage time[15];
c) To request your personal data correction or cancellation[16];

[14] GDPR Art. 15, Right of access by the data subject 1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; (f) the right to lodge a complaint with a supervisory authority; (g) where the personal data are not collected from the data subject, any available information as to their source; (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. 2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer. 3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form. 4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others

[15]GDPR Art.16, Right to rectification: The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

[16] GDPR Art. 17, Right to erasure ('right to be forgotten') 1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1). 2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data. 3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: (a) for exercising the right of freedom of expression and information; (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3); (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or (e) for the establishment, exercise or defence of legal claims.

d) To get the processing restrictions[17];
e) To obtain the portability of data: a data controller receives data in a structured and readable format from another data controller without impediments[18];
f) To object to the processing of your personal information at any time, and in case of direct marketing purposes as well[19];
g) To object to an automated decision making related to natural individuals, including profiling[20];
h) To require the personal data access, rectification, cancellation, restriction or objection, in addition to the right of portability;
i) To withdraw the consent at any time without prejudicing the lawfulness of the processing based on a prior consent; and
j) To lodge a complaint with the Data Controller.

[17] GDPR Art. 18, Right to restriction of processing: 1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; (d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject. 2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State. 3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted; GDPR Art. 19, Notification obligation regarding rectification or erasure of personal data or restriction of processing: The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

[18] GDPR Art. 20, Right to data portability 1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and (b) the processing is carried out by automated means. 2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible. 3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. 4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

[19] GDPR Art. 21 Right to object and automated individual decision-making- Right to object 1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. 2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. 3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes 4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information. 5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications. 6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

[20] GDPR Art. 22, Automated individual decision-making, including profiling
1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. 2. Paragraph 1 shall not apply if the decision: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
(c) is based on the data subject's explicit consent. 3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. 4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

In order to assert these rights, please send a written request, together with the scanning of an identification document, to [---to be completed---] at the following e-mail address [---to be completed---] Requests will be treated with the greatest care to guarantee the effective exercise of one's own rights, within the terms established by the GDPR.

Complaints

Complaints or questions relative to the protection and privacy of data must be addressed to the person in charge of the protection of data, [---to be completed---]; contact e-mail: [---to be completed---]

You will also have the right to make a complaint to the national control authority: [---to be completed---

Attachment 2

SERICS table purpose of processing: scientific research

Purpose of Processing: Scientific Research	Information	Notes
1. Data Controller	Who is?	
2. Data Processor	Who is?	
3. Categories of personal data	- Personal data (art. 4) - Data belonging to special categories (art. 9) - Both data types	Describe the data, sorting them into the corresponding categories
4. Kind of processing	For example Collection, Destruction, Recording, etc.	Briefly describe each planned action
5. Recipients to whom data will be disclosed	For example Partner, etc.	
6. Categories of data subjects to whom the data refer	Choose: - Employees/consultants - Minors - Vulnerable persons (victims of violence or abuse, refugees, asylum seekers) - Citizens - Patients - Participants in research activities - Project stakeholders - Other(please specify)	
7. Place (physical or virtual) of data storage	For example, Room, Office, PC, etc.	
8. Security measures	For example, Office's key, Password, Cryptography, etc.	Describe each measure according to the kind of data, location of storage, recipients and categories of data subjects
9. Transfers of personal data to third countries	Yes/No	If yes, specify: -whether it is a European or third country

Purpose of Processing: Scientific Research	Information	Notes
		-which country it is

NOTES

1) Article 24, co. 1, GDPR: '1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons***, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation***. Those measures shall be reviewed and updated where necessary'

2) Article 28, co. 1, GDPR: '1. ***Where processing is to be carried out on behalf of a controller***, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject'

3) Art.4, co. 1, GDPR: '***personal data*** means 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;

   Art.9, GDPR: "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"

4) Art.4, co. 2, GDPR: '***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'

5) Art. 4, co. 9, GDPR: '***recipient*** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing'

8) Art. 32, GDPR: '***Security of processing***':

   '1. Taking into account 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 controller

and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) the pseudonymisation and encryption of personal data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law'

Attachment 3

SERICS TABLE PURPOSE OF PROCESSING: COMMUNICATION AND DISSEMINATION

Purpose of Processing: Communication and Dissemination	Information	Notes
1. Data Controller	Who is?	
2. Data Processor	Who is?	
3. Categories of personal data	- -Personal data (art. 4) - -Data belonging to special categories (art. 9) - -Both data types	Describe the data, sorting them into the corresponding categories
4. Kind of processing	For example, Collection, Destruction, Recording, etcs.	Briefly describe each action planned
5. Recipients to whom data will be disclosed	For example Partner, etc.	
6. Categories of data subjects to whom the data refer	Choose: - Employees/consultants - Minors - Vulnerable persons (victims of violence or abuse, refugees, asylum seekers) - Citizens - Patients - Participants in research activities - Project stakeholders - Other(please specify)	
7. Place (physical or virtual) of data storage	For example, Room, Office, PC, etc.	
8. Security measures	For example, Office's key, Password, Cryptography, etc.	Describe each measure according to the kind of data, location of storage, recipients and categories of data subjects

9. Transfers of personal data to third countries	Yes/No	If yes, specify: -whether it is a European or third country -which country it is

NOTES

1) Article 24, co. 1, GDPR: '1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons***, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation***. Those measures shall be reviewed and updated where necessary'.

2) Article 28, co. 1, GDPR: '1. ***Where processing is to be carried out on behalf of a controller***, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject'.

3) Art.4, co. 1, GDPR: '***personal data*** means 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;

   Art.9, GDPR: "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'.

4) Art.4, co. 2, GDPR: '***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'.

5) Art. 4, co. 9, GDPR: '***recipient*** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing'.

8) Art. 32, GDPR: '***Security of processing***':

   '1. Taking into account 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 controller

and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) the pseudonymisation and encryption of personal data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law'.

Attachment 4

INFORMATION ON THE TREATMENT OF PERSONAL DATA FOR STAKEHOLDERS

Summary of Information for Stakeholders

We respect the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) hereafter referred to as GDPR[21], and this policy explains how we collect and treat any information that you give us. You will not find any complicated legal terms or long passages of unreadable text. We have no desire to trick you agreeing into something you might later regret.

Our policy covers the following:

- Why we value your privacy;
- How we collect information;
- What information we hold;
- Where we store your information;
- What we use your information for;
- Who is responsible for your information at our company;
- Who has access to information about you;
- The steps we take to keep your information private;
- How to complain; and
- Changes to the policy.

Why we value your privacy:

We value your privacy as much as we do our own, so we are committed to keeping your personal and business information safe. We ask for only the bare minimum from our website's users. We will never use your personal information for any reason other than the reason you gave it, and we will never give anyone access to it unless we are forced to by law.

How we collect information:

We ask for contact information, including your name, e-mail address and phone number, so that we can reply to your enquiry. We ask for your account and contact information when you register for an account or when you will be contacted directly.

[21] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), *OJ L 119, 4.5.2016, p. 1–88*

Occasionally, we might receive your contact information from one of our partners. If we do, we protect it in exactly the same way as if you give it to us directly.

What information do we hold:

When you contact us by e-mail or through our website, we collect your name, e-mail address, phone number and the name of the company you work for (if given).

Where we store your information:

When you contact us by e-mail or through our website, we store your information in our website's data log. When you register for an account at the SERICS Project, your information is stored in our platform. We chose these systems partly for their commitment to security.

What we use your information for:

We occasionally use your contact information to send you details of our events and services. When we do, you have the option to unsubscribe from these communications, and we will not send them to you again.

Who is responsible for your information?

Partners of the SERICS Project who act as data processor for stakeholder data, are responsible for the security of your information. You can contact them if you have any concerns about the information we store.

Who has access to information about you?

When we store information in our own systems, only the people who need it will have access to it. The data is shared with project partners for project-related activities.

The steps we take to keep your information private:

When we store your information in third-party services, we permit access only to people who need it. Passwords are encrypted.

How to complain:

We take complaints very seriously. If you have any reason to complain about the ways in which we handle your privacy, please contact [---to be completed---]:

- The controller for [---to be completed---]is [---to be completed---].; contact e-mail: [---to be completed---].
- The internal person in charge of processing data for [---to be completed---]. is [---to be completed---; contact e-mail: [---to be completed---];

Changes to the policy:

In case of changes in the contents of this policy, those will be in force after being shared with the SERICS partners and approved.

Attachment 5

INFORMED CONSENT FOR STAKEHOLDERS

Privacy Control

SERICS will use the information you provide on this form to keep in touch with you and to provide updates.

Occasionally, we will use your contact information to send details of our events and services.

We have to specify that when we do, you have the option to unsubscribe from these communications, and we will not send them to you again.

Please let us know all the ways you would like to hear from us and use your data. You are able to edit your account data anytime.

Can we use your data?

- Yes, you can use my details.
- No, I don't agree.

Do you agree with our privacy policy?

- Yes, and I have read the privacy policy.
- No, I don't agree.

See Attachment 1 of the SERICS Personal Data Policy for more information on the use of your personal data, in compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)[22].

[22] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), *OJ L 119, 4.5.2016, p. 1–88*

Attachment 6

INFORMED CONSENT FOR SPEAKERS INVITED TO CONVENTIONS AND EVENTS

Name and Surname: [---to be completed---]

Institution: [---to be completed---]

The undersigned person, [---to be completed---] , born in [---to be completed---], on [---to be completed---], as speaker for the Conference entitled '[---to be completed---] Conference', which will be held on [---to be completed--- dd/mm/yyyy], at the [---to be completed---], [---to be completed---], in conformity with and for the effects of Article 13 and other relevant articles of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) hereafter referred to as GDPR[23,24] that contain dispositions for the protection of persons and of other subjects with regard to the processing of personal data, as well as with the signing of the present form,

CONSENTS TO

[23] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), *OJ L 119, 4.5.2016, p. 1–88*

[24] GDPR Art. 13, Information to be provided where personal data are collected from the data subject: 1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;(b) the contact details of the data protection officer, where applicable;(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available. 2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; (c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; (d) the right to lodge a complaint with a supervisory authority; (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. 3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2. 4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

the following: (a) the collection of personal data; (b) the collection of photographs and videos for transmission and publication by means of streaming, as realised during the events of the project; (c) the collection of presentations, slides, etc., as utilised by the undersigned spokesperson during his or her own presentation at Project events; and (d) the publication of the data and documents on the website of the above-indicated [---to be completed---] Conference.

The writer has been informed that the data processing mentioned above will be carried out for the following purposes: (1) promoting the [---to be completed---] Conference; (2) publishing the documents of the Conference; and (3) supplying services connected with the [---to be completed---] Conference.

In order to realise the aims stated above, the undersigned authorises the organisers of [---to be completed---] Conference to collect and communicate personal data to external subjects or potential sponsors who will provide attestations of participation, in addition to updating the website of the [---to be completed---] Conference.

The opposition of the signature constitutes a declaration of an examination of the information regarding the processing of personal data as well as the authorisation of the processing performed by the person responsible. Such processing is authorised for the purposes and following the procedures described above.

Read, confirmed and signed

[---to be completed---] (Place),

on [---to be completed--- dd/mm/yyyy] (Date)

[---to be completed---] Signature of the declarant

Attachment 7

INFORMED CONSENT OF CONVENTIONEERS/PERSONS ATTENDING EVENTS

Request for registration for the [---to be completed---] Convention and consent to the processing of personal data

Name and Surname: [---to be completed---]

Qualification/Function: [---to be completed---]

Institute of affiliation: [---to be completed---]

Address of the organisation: [---to be completed---]

Telephone: [---to be completed---]

E-mail: [---to be completed---]

Passport or identity card number (EU and third-world countries): [---to be completed---] (Address, Country)

The undersigned [---to be completed---]

born in [---to be completed---] on [---to be completed--- dd/mm/yyyy] Fiscal Code [---to be completed---], in his/her/their capacity of [---to be completed---], and in conformity with and for the effect of Article 13 and other relevant articles of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) hereafter referred to as GDPR[25,26] setting dispositions to

[25] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), *OJ L 119, 4.5.2016, p. 1–88*

[26] GDPR Art. 13, Information to be provided where personal data are collected from the data subject: 1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;(b) the contact details of the data protection officer, where applicable;(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available. 2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; (c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; (d) the right to lodge a complaint with a supervisory authority; (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those

safeguard persons and other subjects with regard to the processing of personal data, as well as with the signature of the present form,

CONSENTS TO

the following: (a) the collection of personal data, photographs and videos made for processing by means of streaming, as realised during the event; (b) the collection of e-mail and other contact data; (c) the publication of data and documents, as per points (a) and (b), on the website of the above-indicated Conference/Seminar/Event [---to be completed---].

The writer has been informed that the processing of data will be carried out for the following purposes: (1) realising and promoting the Conference/Seminar/Event, entitled [---to be completed---], within the ambit of the project [---to be completed---]; (2) publishing the documents of the Conference/Seminar/Event; and (3) supplying services connected with the Conference/Seminar/Event.

For the purposes narrated above, the undersigned authorises the organisers to collect and communicate the personal data to other subjects, such as possible sponsors or external subjects who will realise testimonials of participation, in addition to updating the website of the Conference/Seminar/Event.

The opposition of the signature constitutes a declaration of an examination of the information regarding the processing of personal data as well as the authorisation of the processing performed by the person responsible. Such processing is authorised for the purposes and with the procedures described above.

Read, confirmed and signed:

[---to be completed---] (Place),

on [---to be completed--- dd/mm/yyyy] (Date)

[---to be completed---]Signature of the declarant

cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. 3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2. 4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.