D8.1 SYNERGISE Ethics and Privacy Handbook

Date
30.04.2024

Author: Pablo Cerezo Martínez, Flavia Roteda Ruffino, Francisco J. Castro-Toledo
Organisation: PLUSETHICS

Co-funded by the European Union

D8.1SYNERGISE Ethics and Privacy Handbook

Grant Agreement	101121321
Call identifier	HORIZON-CL3-2022-DRS-01
Project full name	SYNERGISE : A novel integrated SYstem of Systems streNgthening tEchnical and logistical capacities to ensure better Response to emerGencies by synergISticallyaddrEssing FRs capability gaps
Due Date	30/04/2024
Submission date	30/04/2024
Project start and end	01.09.2023 – 28.02.2027
Authors	Pablo Cerezo Martínez, Flavia Roteda Ruffino, Francisco J. Castro-Toledo
Lead Beneficiary	PLUSETHICS

About the document

The SYNERGISE Ethics and Privacy Handbook sets standards for security research and enhances first responder capabilities, emphasising ethical research and privacy. It addresses issues such as human participation, AI ethics and privacy, and ensures ongoing compliance and oversight. Annexes provide tools for informed consent and ethics and privacy protocols. Overall, it is a benchmark for ethical integrity that responsibly advances emergency response capabilities.

Document revision history

Version	Issue & Date	Reviewer name, Beneficiary short name	Date of approval
0.1	15/03/2024	PLUSETHICS	12/03/2024
0.2	12/04/2024	PLUS ETHICS	12/04/2024
1.0	23/04/2024	PLUS ETHICS	23/04/2024

Acknowledgment

The project is jointly funded from the European Union's Horizon Europe research and innovation programme; State Secretariat for Education, Research, and Innovation from Switzerland, R2 Network from the United States of America, the Japan Science and Technology Agency, the Korea Ministry of Science and ICT, and the Korea Electronics and Telecommunications Research Institute.

Nature of the deliverable[1]		R

Dissemination level

PU	Public, fully open. e.g., website	✓
SEN	Sensitive, limited under the conditions of the Grant Agreement	
CL	Classified information under the Commission Decision No2015/444	

[1] Deliverable types:
R: document, report (excluding periodic and final reports). DEM: demonstrator, pilot, prototype, plan designs.
DEC: websites, patent filings, press and media actions, videos, etc. OTHER: software, technical diagrams, etc.

Table of contents

List of tables

Abbreviations

FRs	First responders
GDPR	General Data Protection Regulation
EU	European Union
EthSR	Ethics Summary Report
EC	European Commission
AI	Artificial Intelligence
ALTAI	Assessment List for Trustworthy Artificial Intelligence
AI HLEG	High-Level Expert Group on Artificial Intelligence
FFP	Fabrication, falsification, or plagiarism
DPIA	Data Protection Impact Assessment (DPIA)
R+D	Research and Development
FRA	European Union Agency For Fundamental Rights
HLRN	Housing and Land Rights Network

Executive summary

The D8.1 SYNERGISE Ethics and Privacy Handbook represents a foundational document for the SYNERGISE project, which aims at enhancing the technical and logistical capacities of First Responders (FRs) through an integrated system of systems approach. Jointly funded by the European Union's Horizon Europe research and innovation program and other international partners, SYNERGISE sets a precedent for ethical and privacy standards in security research and innovation.

Objectives and Scope
The handbook outlines the collective values and commitments of the SYNERGISE consortium, guiding actions and decisions to ensure ethical behavior, privacy rights protection, legal compliance, risk mitigation, and a culture of accountability and transparency. It serves not only as a framework for promoting ethical conduct but also as a tool for enhancing the consortium's cohesion, reputation, and the overall effectiveness of the research undertaken.

Ethical Framework
Adhering to European standards of Responsible Research and Innovation, SYNERGISE is committed to nine primary ethical principles: respect for human dignity and integrity; honesty and transparency towards research subjects; respect for individual autonomy; protection of vulnerable individuals; privacy and confidentiality assurance; promotion of justice and inclusiveness; harm minimization and benefit maximization; equitable benefit sharing; and environmental respect.

Key Ethical Issues
The handbook addresses ethical issues specific to SYNERGISE, including human participation, non-discrimination, and equality, with a particular focus on voluntary informed consent, protection of autonomy, beneficence, non-maleficence, and justice. It also emphasizes the importance of gender equality, respect for sexual orientation, and disability rights within the project's framework. On the other hand, given the role of AI in emergency response, SYNERGISE adopts the Ethics Guidelines for Trustworthy Artificial Intelligence, focusing on recommendations for implementing these ethical requirements underline the consortium's commitment to responsible use of AI.

Data protection and Privacy framework
Legal frameworks like the General Data Protection Regulation (GDPR) ensure proper data handling, emphasizing informed consent and security measures. These reforms position the EU as a leader in global data protection. The SYNERGISE project seeks to enhance awareness and understanding of data protection rules, particularly for non-specialist legal practitioners, reflecting the EU's commitment to upholding privacy rights in an evolving digital landscape.

Governance and Implementation
The governance structure facilitates ethical decision-making, addressing emerging concerns and ensuring consortium partners are well-versed in ethical practices. Training sessions and webinars are mandated for raising awareness, and a protocol for human participation in research activities highlights risk assessment, informed consent, confidentiality, data protection, and inclusion policies.

Continuous Review and Updates

Recognizing the dynamic nature of ethical standards, the handbook advocates for periodic reviews and updates to stay abreast of changes in legal, technological, and societal landscapes. This ensures SYNERGISE's ethical practices remain relevant and effective, demonstrating a commitment to ethical excellence and societal well-being.

Annexes

This deliverable includes a template for obtaining informed consent from participants in research activities and an ethics protocol for safety research involving human participation. The consent template covers project details, risks, confidentiality, and contact information, ensuring participants' understanding and voluntary consent. The ethics protocol assesses risks, handles personal data, and addresses ethics concerns during research involving humans, ensuring compliance with data protection regulations like GDPR within the EU. It serves as a crucial resource for researchers, respecting participants' rights, and dignity.

In conclusion, the D8.1 SYNERGISE Ethics and Privacy Handbook sets a comprehensive and robust framework for ethical integrity, privacy protection, and responsible research within the security domain. It not only adheres to existing legal and ethical standards but also sets a benchmark for future initiatives, showcasing a profound commitment to advancing emergency response capabilities in an ethically responsible manner.

1. Introduction

1.1. Objectives

When we elaborate an ethics and privacy handbook, whether it is a general one or, as in this case, one specifically tailored for security research within the SYNERGISE project, we are talking about a document that explicitly articulates the values of a company or organisation. In this context, it includes the principles shared by all members of the SYNERGISE consortium and the commitments they have made to guide their actions. This handbook serves as a tangible demonstration of the guiding values that shape the behaviour of SYNERGISE partners and influence their decision-making processes. It presents several advantages that distinguish organisations with such policies from those without.

The objectives of such a document include:

1. To provide guidance on ethical behaviour.
2. Protect privacy rights.
3. Ensure legal compliance.
4. Mitigate risk.
5. Promote accountability and responsibility.
6. Promote transparency and trust.
7. Facilitate education and training.
8. Allow for adaptation and evolution.

In addition, there are several key benefits associated with the implementation of such a handbook:

1. Promotes greater cultural cohesion within the consortium.
2. Enhance the reputation of the consortium.
3. Reduce the likelihood of criminal or anti-social behaviors among members.
4. Promote mutual respect, equality, inclusiveness, and legitimacy within the consortium.
5. Increase the motivation and satisfaction of those committed to upholding the code of ethics.

In line with these objectives and benefits, this document aims to summarise the primary and most relevant standards of conduct necessary for ethical research practices within the security domain of SYNERGISE. It does so from a non-dogmatic standpoint, ensuring alignment with the prevailing social, normative, and ethical contexts. The goal is to ensure that all individuals involved in SYNERGISE activities always demonstrate professional and ethical behaviors. This not only fosters internal and external commitment, but also encourages members to report any behaviors that may damage the Consortium's image or reputation.

1.2. Scope of application of the SYNERGISE Ethics and Privacy Handbook

The scope and application of such a document may vary depending on the type of research, the number of participants, the organisations involved in the research process, etc. However, in the case of the SYNERGISE Ethics and Privacy Manual, it is necessary to make a clear distinction between the different areas of application of the document. In this sense, there are four essential aspects that make up the scope of this handbook. In particular, the following can be highlighted and emphasized:

1. The scope of this document extends to the SYNERGISE consortium partners.
2. The different activities to be carried out by the consortium partners.
3. About the specific participants requiring more detailed regulation, not directly related to security research, they are all subject to sectoral codes and manuals contained in the SYNERGISE PROPOSAL documents or internal documents of the SYNERGISE partners.
4. The content of this SYNERGISE Handbook will always be applied in a coherent manner and in accordance with the content of European documents that are mandatory in the conduct of research. All of these are the result of the efforts and commitment made by organisations within society at an ethical and regulatory level.

It is imperative that the persons subject to this document both know and comply with its contents and contribute to facilitate its implementation in the research activities of the SYNERGISE project, including in any case the communication of any violation that comes to their attention. In this sense, the persons subject to this document will maintain a collaborative and responsible attitude in identifying situations of actual or potential breaches of the ethical principles and rules of conduct contained in this document. On the contrary, failure to comply with the Code may result in the application of the sanctions regime established in the applicable labour regulations, without prejudice to any administrative or criminal sanctions that may be applicable.

2. SYNERGISE Ethics & Privacy Framework

SYNERGISE has outlined, in line with the main European standards of Responsible Research and Innovation, 9 main ethical principles that guide its research activities.

- Respecting human dignity and integrity;
- Ensuring honesty and transparency towards research subjects;
- Respecting individual autonomy and obtaining free and informed consent (as well as assent whenever relevant);
- Protecting vulnerable individuals;
- Ensuring privacy and confidentiality;
- Promoting justice and inclusiveness;
- Minimising harm and maximising benefit;
- Sharing the benefits with disadvantaged populations, especially if the research is being carried out in developing countries;
- Respecting and protecting the environment and future generations.

All these principles, which are binding on all partners, are closely aligned with the following reference documents:

- Regulation (EU) 2021/695 establishing Horizon Europe — the framework programme for research and innovation, laying down its rules for participation and dissemination
- Directive (EU) 2016/679 General Data Protection Regulation;
- SYNERGISE proposal approved (from the SYNERGISE Grant Agreement and Consortium Agreement);
- EU Grants: How to complete your ethics self-assessment: V2.0 – 13.07.2021;
- EU grants: Classification of information in Horizon Europe projects: V1.0 – 22.07.2021;
- EU Grants: How to handle security-sensitive projects: V1.0 – 01.07.2021;
- Ethics Advisor and Ethics Advisory Boards: v2.0 – 15.02.2023;
- Horizon Europe - Ethics Advisor / Ethics Advisory Board Report - Version 1.5 - March 2023;
- European Textbook on Ethics in Research;
- Ethics for researcher – Facilitating Research Excellence (European Commission);
- The European Code of Conduct for Research Integrity;
- Ethics in Social Science and Humanities (European Commission);
- Research, risk-benefit analysis and ethical issues (European Commission);
- Guidance to facilitate the implementation of targets to promote gender equality in research and innovation (European Commission);
- Horizon Europe guidance on gender equality plans (European Commission).

2.1. Key ethics issues in SYNERGISE

This section details the ethical principles that are of particular relevance in the research context of the SYNERGISE project. In order to identify the requirements, a distinction has been made between key and secondary ethics issues. This distinction is based on what is stated in the Ethics Summary Report (EthSR). where the four main ethical categories affecting the SYNERGISE project are identified by de EC ethics panel, namely: humans, artificial intelligence, personal data and third countries. On the other hand, it is also worth mentioning a number of ethical principles and recommendations which, although they do not have the character of "main", are necessary to be taken into account for the correct ethical development of the research and which, in addition, provide the project with a broader and more complete ethical framework. For this reason, although they do not have the same specific relevance as the first principles, they are important in the context of the research to be carried out as a whole. As noted above, the following principles, as shown in the diagram, will be taken into account in determining the primary ethical principles.

2.1.1. Human participation

Firstly, it is very important to determine what human participation is and will look like in the context of SYNERGISE[2]. In this respect, following the guideline on serious and complex ethics issues in EU-funded research launched by European Commission:

> 'Humans must be considered as 'research participants' whenever they are recruited, observed, actively engaged, or in any other way may be influenced, manipulated, or directed by the research. Regardless of the nature, methods, or topic of the proposed research activities (e.g., collecting biological samples, using personal data, medical interventions, interviews, observations, tracking etc.), ethical issues may arise in any research involving humans'[3].

With a view to participation with humans in the context of the activities to be carried out, it is recommended that the following considerations be considered:

- The respect for persons and for human dignity.
- Fairness understanded as: Fair distribution of benefits and burden and the commitment to countering bias, discrimination, and stigmatisation in all stages of the SYNERGISE project.
- All the necessary practices should be in constant correspondence with legal local, national, and international demands.
- The rights and interests of the participants.
- The need to ensure participants' free informed consent (with particular attention to vulnerable categories of individuals such as children, patients, discriminated people, minorities, persons unable to give consent, etc.)[4].

Autonomy, Non-Maleficence, Beneficence and Justice

One of the fundamental pillars on which human participation is established must be respect for the principles of autonomy, non-maleficence, beneficence, and distributive justice. In this respect, no-one is obliged to participate in research. You need to justify why human participation in your planned work is necessary in the first place. Anyone who considers participating in your research must have a fair chance to judge whether it is worthwhile taking the time and making the effort to

2 In this regard, it should be noted that the expected human participation will be carried out mainly by FRs and (conditionally) victims in the affected area.
3 European Commission (2021): *Identifying serious and complex ethics issues in EU-funded research*, p.5.
4 European Commission (2021): *How to complete your ethics self-assessment*, p. 8.

share information with you. Your research involves human participants if you are recruiting them or actively involving or influencing, manipulating, or directing them in any way in your research activities5.

Thus, in this sense, those projects that require human participation: requires evidence of the voluntary, free, and informed consent of those who contribute their time, insights, effort and data for the use of researchers6. Even though, it is peremptory to stress that the obtention of informed consent does not in itself ensure ethical research. Moreover, as the EU points out: this very act and the aim of safeguarding participants' rights and well-being in the research setting may place them at risk of harm in their social context (rather than affording them protection)7. For this reason, it is quite important to describe the procedures for obtaining written informed consent. In this regard, deliverable 9.2.1. about Data Protection Impact Assessment Report described how the consent to participate in the project will be collected, processed, and stored (including confidentiality and data minimization) in compliance with ethic regulations and especially the General Data Protection Regulation (GDPR), which came into effect in all EU member states May 25, 2018. The latter implies that personal data will be anonymized unless such anonymization would be incompatible with the envisioned research activities. In such case, other privacy-preserving techniques – such as encryption or pseudonymization – will be maintained.
On the other hand, in view of the principle of respect for autonomy and for the purpose of preparing informed consents, a careful review of the following points is recommended:

- Give participants a clear explanation of the aims, overall purpose, methods, and implications of the research.
- Explain that participation is voluntary.
- Remind participants that they have a right to withdraw their consent at any time without any consequences.
- Explain the degree of benefit, risks, burden, or discomfort involved in participation. Give an estimate of the time and effort expected of participants.
- Explain precautions to ensure participants' safety and provide information on insurance if there is any.
- Explain who is funding the research and for what purpose.
- Disclose who will benefit from the research.
- Give a firm commitment to protecting respondents' anonymity and privacy (provided that this can genuinely be guaranteed).
- Make a clear commitment to treating personal and sensitive information confidentially. Reassure participants that there are secure procedures for analysing any data gathered.
- Explain clearly who access to any data will have that participants provide.
- Consider any unintended/unexpected/incidental findings and explain how you intend to deal with such findings.
- Explain briefly where research findings will be published.
- Offer to provide respondents with further information about research if they ask for it.
- Give the name and contact details of the contact person who can answer any queries participants may have.
- Clarify possible uses to which data may be put in future (if this is envisaged) and clarify whether participants will be asked for consent again if this is the case. Cover any issues relating to copyright of data and other materials used in the research8.

On the other hand, with regard to the principles of non-maleficence, beneficence and justice, it is convenient to pay attention to the following issues that can be considered as problematic in the

[5] European Commission (2021): *Ethics in social sciences and humanities*, p. 11.
[6] European Commission (2021): *Ethics in social sciences and humanities*, p. 13.
[7] European Commission (2021): *Ethics in social sciences and humanities*, p. 13.
[8] European Commission (2021): *Ethics in social sciences and humanities*, pp. 13-14

activities with human participation that can be carried out within the context of the SYNERGISE project in order to establish preventive or reactive mitigation or avoidance measures:

- Involves highly vulnerable participants, such as people exposed to or affected by multiple or intersecting vulnerabilities (e.g., refugees or migrants facing extreme poverty, gender-based stigmatisation, or violence), or methods that have the potential to significantly exacerbate the vulnerability of already vulnerable groups or individuals; or
- Suggests the potential coercion of research participants through excessive or inappropriate financial compensation, or because their relationship to the researchers suggests that their consent may be obtained under some form of duress or out of a sense of obligation.
- Uses high-risk or inappropriate techniques and methods that may expose participants to unacceptable risk (e.g., insecure online surveys addressing sensitive issues or processing sensitive/special category data, methods that encourage participation by vulnerable groups without regard to their vulnerability); or
- Involves studies whose findings carry a high risk of exposure or identification of individuals and/or stigmatisation of a minority or marginalised group (e.g., based on poverty, ethnicity, religion, gender/gender identity, disabilities, age, sexuality or perceived involvement in illegal activities).
- Has the potential to result in significant harm to the participants (or researchers), such as significant physical pain or bodily harm not related to simple routine medical procedures (e.g. taking a blood sample), psychological harm, personal embarrassment or humiliation, or other harm that may adversely affect the participants in a significant way9.

Non-Discrimination

Discrimination occurs when one person is treated less favourably than another by virtue of his or her gender, sex, race, colour, ethnic or social origin, genetic features, language, religion, or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation10. Because discrimination can be present in many ways and levels, this is one of the fundament ethical requirements that should be present at all stages of the project. SYNERGISE partners should consider the following different ethical issues:

Gender and racial discrimination

SYNERGISE partners promote gender equality in research and innovation projects, in this case also within SYNERGISE. SYNERGISE is committed to the latest policies developed by the European Institute for Gender Equality, which may be found in several documents (such as Guidance to facilitate the implementation of targets to promote gender equality in research and innovation11, the Gender Equality Strategy 2020-202512 or the HORIZON 2020 Programme AGA-Annotated Model Grant Agreement, where article 33 of the fourth section specifies the obligation to aim for gender equality13) where a plan of gender, racial and ethnic equality is established under a double perspective: gender, racial and ethnic policies applied to all; and gender policies applied to research participants.

In this regard it is relevant to stress the following related to possible research participants:

---

[9] For the aim of this deliverable, only those topics that can be related to SYNERGISE possible potential issues have been mentioned. European Commission (2021). *Identifying serious and complex ethics issues in EU-funded research*, p.6.

[10] FRA (2018). *Handbook on European non-discrimination law*. Luxembourg: Publications Office of the European Union. Available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-handbook-non-discrimination-law-2018_en.pdf ; Article 14 from ECHR concerning prohibition of discrimination. Available at: https://www.equalityhumanrights.com/human-rights/human-rights-act/article-14-protection discrimination#:~:text=The%20enjoyment%20of%20the%20rights,association%20with%20a%20national%20minority%2C ; Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin. Available at: https://eur-lex.europa.eu/eli/dir/2000/43/oj This is also a fundamental right enshrined in the Charter of Fundamental Rights of the European Union, article 21. European Parliament (2000). *Charter of Fundamental Rights of the European Union*. Available at: https://www.europarl.europa.eu/charter/pdf/text_en.pdf

[11] European Commission & Helsinki Group on Gender in Research and Innovation. Guidance to facilitate the implementation of targets to promote gender equality in research and innovation, 2018. Luxembourg: Publications Office of the European Union.

[12] European Commission (2020). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Union of Equality: Gender Equality Strategy 2020-2025

[13] European Commission (2019). HORIZON 2020, H2020 Programme, AGA- Annotated Model Grant Agreement, p.268

- The selection processes for research participants will not be affected by the gender, gender identity, sex or sexual orientation of potential participants. These variables will only be an exclusion variable in the investigations which require it specifically in order to answer to widely justified objectives.
- In case of remuneration for the participation of the individuals in researching, it will be completely equitable.
- And related to dissemination plan:
  These measures are adopted to grant men and women equal opportunity access between and to avoid gender discrimination.
- Equal numbers of women and men in outreach activities such as conferences or workshops should be ensured.

Sexual orientation

According to the *Yogyokarta Principles,* sexual orientation can be understood to refer to each person's capacity for profound emotional, affectional and sexual attraction to, and intimate relations with, individuals of a different gender or the same gender or more than one gender.14 In this regard, SYNERGISE partners have to ensure that any less-favorable treatment[15] of individuals due to their sexuality will not be tolerated and will be denounced.

- Are there measures in place to ensure that there is no discriminatory treatment on the basis of the sexual status of individuals who may be part of the SYNERGISE project?
- Are there ways in which unequal treatment on the basis of sex can be reported?

Disability

In the context of SYNERGISE project, the rights of persons with disabilities must be ensured. According to European Commission, persons with disabilities have the right to protection from any form of discrimination and violence, equal opportunities in and access to justice, education, culture, housing, recreation, leisure, sport and tourism, and equal access to all health services[16.] Moreover, the Commission has expressed their commitment in the following aspects[17]:

- Working with Member States to implement the 2000 Hague Convention on the international protection of vulnerable adults in line with the UNCRPD, including by way of a study on the protection of vulnerable adults in cross-border situations, notably those with intellectual disabilities, to pave the way for its ratification by all Member States
- Launching a study on procedural safeguards for vulnerable adults in criminal proceedings and assessing the need for legislative proposals strengthening the support and protection of vulnerable adults who fall victims of crime, in line with the EU Victims' Rights Strategy (2020-2025).

Concerning equal access to social protection, healthcare, education and goods and services including housing, the Commission calls on Member States to[18]:

[14] The Yogyakarta principles plus 10 (2017). *Additional principles and state obligations on the application of international human rights law in relation to sexual orientation, gender identity, gender expression and sex characteristics to complement the yogyakarta principles*. Geneva. For more information concerning sexual orientation see also: International Commission of jurist (2009). *Sexual Orientation, Gender identity and International Human Rights Law- Practitioners Guide N°4*. Geneva. Available at: https://www.refworld.org/pdfid/4a783aed2.pdf ; United Nations Human Rights (2019). Born free and equal. *Sexual orientation, gender identity and sex characteristics in international Human Rights Law*. Available at: https://www.ohchr.org/Documents/Publications/Born_Free_and_Equal_WEB.pdf

[15] In this regard see: European Union Agency For Fundamental Rights (FRA)(2014) . *EU LGTB survey. European Union lesbian, gay, bisexual and transgender survey*. Main results. Luxembourg: Publication Office of the European Union.

[16] European Commission (2021). *Union of Equality. Strategy for the rights of persons with Disabilities 2021-2030*, p. 16. Luxembourg: Publications Office of the European Union. Concerning rights of disable people and demands see also: European Commission (2018). *Combatting disability discrimination and realising equality. A comparison of the UN Convention on the Rights of Persons with Disabilities and EU equality and non-discrimination law*. Luxembourg. Publications Office of the European Union; and the Convention on the Rights of Persons with Disabilities. Available at: https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html

[17] European Commission (2021). pp.16-17.

[18] European Commission (2021). p.17.

- Enable the adoption of the Commission proposal for a horizontal directive on implementing the principle of equal treatment outside the field of employment including disability.
- Support cooperation between the EU and the national UNCRPD frameworks and members of European networks of rights defenders.

Social origin, birth and property

Despite the fact that given the specifications of the SYNERGISE project this type of ethical problems are unlikely to occur, it is advisable to take into consideration that, in their work concerning researching, implementation, dissemination etc., must ensure that different features such as social origin, economic aspects, birth and property do not pose any barriers in the normal development of the project.

According to the Committee, 'social origin', 'birth' and 'property' statuses are interconnected. Social origin 'refers to a person's inherited social 'statuses. It may relate to the position that they have acquired through birth into a particular social class or community (such as those based on ethnicity, religion, or ideology), or from one's social situation, such as poverty and homelessness. Additionally, the ground of birth may refer to one's status as born out of wedlock or being adopted. The ground of property may relate to one's status in relation to land (such as being a tenant, owner, or illegal occupant), or in relation to other property[19].

Permissible scope of differential treatment

There may be situations where different treatment is required even considering the anti-discrimination recommendations set out above. In such cases, according to the United Nations:

> "Differential treatment based on prohibited grounds will be viewed as discriminatory, unless the justification for differentiation is reasonable and objective[20]. This will include an assessment as to whether the aim and effects of the measures or omissions are legitimate, compatible with the nature of the Covenant rights and solely for the purpose of promoting the general welfare in a democratic society. In addition, there must be a clear and reasonable relationship of proportionality between the aim sought to be realised and the measures or omissions and their effects. A failure to remove differential treatment on the basis of a lack of available resources is not an objective and reasonable justification unless every effort has been made to use all resources that are at the State party's disposition in an effort to address and eliminate the discrimination, as a matter of priority"[21].

On the other hand, according to the European Fundamental Rights Agency, the following can be demonstrated to justify different treatment:

- That the rule or practice in question pursues a legitimate aim.
- That the means chosen to achieve that aim (that is, the measure which has led to the differential treatment) is proportionate to and necessary to achieve that aim[22].
- There is no other means of achieving that aim that imposes less of an interference with the right to equal treatment. Put otherwise, that the disadvantage suffered is the minimum possible level of harm needed to achieve the aim sought.
- The aim to be achieved is important enough to justify this level of interference[23].

[19] European Commission (2018). *Handbook on European non-discrimination law*, p.218.
[20] Regarding this, one of the specifications of the SYNERGISE project is related to the physical requirements for field operations. In this sense, permissible scope of different treatment will be justified.
[21] United Nations (2009). Economic and Social Council. Committee on economic, social and cultural rights. General Comment N° 20. *Non-discrimination in economic, social and cultural rights* (art 2, para.2, of the International Covenant on Economic, Social and Cultural Rights) p.5.
[22] FRA (2018). *Handbook on European non-discrimination law*.p.93
[23] FRA (2018). *Handbook on European non-discrimination law*.p.93

Particular actions in the context of FRs operations to preserve the Human Right to Health

Due to the particularities of SYNERGISE, FRs may have to face critical situations. In this regard, their actions related to relief, rehabilitation, reconstruction, and recovery efforts have to pay attention on the following considerations:

- The needs of affected persons requiring medical care, including mental health and psychosocial care, whether the problems and needs are pre-existing, emergency-induced or related to the humanitarian response.
- The health needs of women and girls, including access to health services and the provision of priority sexual and reproductive health services, including actions to prevent maternal morbidity and mortality, prevent and clinically manage cases of sexual violence, and prevent HIV; provision of appropriate medication and hygienic supplies; access to reproductive and specialized health services; including family planning and emergency obstetrical care.
- The prevention of, response to, and mitigation of, contagious and infectious diseases, including HIV/AIDS, among the affected population.
- The need for specialized services required for injured persons and persons with disabilities.
- The health needs of persons with chronic illnesses. • Community-based psychosocial support.
- Specialized mental health services, as needed, for those among affected persons with mental disorders.
- Providing sufficient female doctors, healthcare staff and interpreters.
- Addressing the problem of alcohol and other substance use in the aftermath of disasters[24].

[24] HLRN (2015). Protecting Human Rights in Disaster Response: Guidelines for State and Non-state Actors, p.9

2.1.2. Artificial Intelligence (AI)

In today's rapidly evolving first responders' technological landscape, Artificial Intelligence (AI) holds immense promise for innovation and progress across various sectors. However, along with its potential benefits come significant ethical and privacy concerns. Recognizing the need for guidelines to navigate these challenges, the High-Level Expert Group on Artificial Intelligence (AI HLEG) introduced the Ethics Guidelines for Trustworthy Artificial Intelligence (AI) in April 2019. This framework outlined seven key requirements, including human agency, transparency, privacy, and accountability, among others, to ensure the development and deployment of Trustworthy AI[25].

Building upon these guidelines, the AI HLEG presented the final Assessment List for Trustworthy Artificial Intelligence (ALTAI). ALTAI translates the abstract principles of Trustworthy AI into a practical and dynamic checklist, facilitating the implementation of ethical standards in AI practices. Through ALTAI, SYNERGISE's developers and deployers can assess the extent to which their AI systems align with ethical principles and identify areas for improvement. By promoting transparency, technical robustness, privacy, and other essential facets of Trustworthy AI, ALTAI endeavors to mitigate risks and safeguard users from potential harm. Ultimately, this handbook on ethics and privacy within the SYNERGISE project will leverage ALTAI's insights to inform recommendations for identifying and managing AI-related risks, ensuring that innovation in AI is pursued responsibly and ethically. Below are some recommendations for each of the seven ethical requirements of the ALTAI[26].

Human agency and oversight

Requeriment	Recomendations
AI systems should empower human beings, allowing them to make informed decisions and fostering their fundamental rights. At the same time, proper oversight mechanisms need to be ensured, which can be achieved through human-in-the-loop, human-on-the-loop, and human-in-command approaches	1. Incorporate a process where end-users and/or subjects are adequately made aware that an AI-system influenced the decision, content, advice or outcome. 2. Ensure that the end-users or subjects are adequately informed that they are interacting with an AI system. 3. Put in place procedures to avoid that end users over-rely on the AI system. 4. Put in place any procedure to avoid that the system inadvertently affects human autonomy. 5. Take measures to deal with the possible negative consequences for end-users or subjects in case they develop attachment. In particular, provide means for the user to have control of the interactions. 6. Take measures to minimize the risk of addiction by involving experts from other disciplines such as psychology and social work. 7. Take measures to mitigate the risk of manipulation, including providing clear information about ownership and aims of the system, avoiding unjustified surveillance, and preserving autonomy and mental health of users. 8. Give specific training to humans (human-in-the-loop, human-on-the-loop, human-in-command) on how to exercise oversight. 9. Establish detection and response mechanisms in case the AI system generates undesirable adverse effects for the end-user or subject. 10. Deploy a "stop button" or procedure to safely abort an operation when needed.

Table 1. *Human agency and oversight ethics recommendations*

[25] It's important to note that the ethics recommendations derived from the proper application of ALTAI are fully compatible with the AI ACT. This legislation will lay the groundwork for AI regulation in the EU, reflecting the ethical principles and privacy concerns addressed in the SYNERGISE project guidelines. More about the ALTA web-based tool in https://digital-strategy.ec.europa.eu/es/node/806

[26] See https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Technical robustness and safety

Requeriment	Recommendations
AI systems need to be resilient and secure. They need to be safe, ensuring a fall back plan in case something goes wrong, as well as being accurate, reliable and reproducible. That is the only way to ensure that also unintentional harm can be minimized and prevented	1. Define risk, risk metrics and risk levels of the AI system in each specific use case. 2. Identify the possible threats to the AI system (design faults, technical faults, environmental threats) and the possible resulting consequences. 3. Assess the risk of possible malicious use, misuse or inappropriate use of the AI system. 4. Assess the dependency of critical system's decisions on its stable and reliable behaviour. 5. Assess the dependency of critical system's decisions on its stable and reliable behaviour. 6. Plan fault tolerance via, e.g., a duplicated system or another parallel system (AI-based or "conventional"). 7. Develop a mechanism to evaluate when the AI system has been changed enough to merit a new review of its technical robustness and safety. Develop a mechanism to evaluate when the AI system has been changed enough to merit a new review of its technical robustness and safety. 8. Put in place measures to ensure that the data (including training data) used to develop the AI system is up to date, of high quality, complete and representative of the environment the system will be deployed in. 9. Put in place a series of steps to monitor and document the AI system's accuracy. 10. Consider whether the AI system's operation can invalidate the data or assumptions it was trained on, and how this might lead to adversarial effects (e.g. biased estimators, echo chambers etc.) 11. Put in place processes to ensure that the level of accuracy of the AI system to be expected by end-users and/or subjects is properly communicated. 12. Put in place a well-defined process to monitor if the AI system is meeting the goals of the intended applications. 13. Test whether specific contexts or conditions need to be taken into account to ensure reproducibility. 14. Put in place verification and validation methods and documentation (e.g. logging) to evaluate and ensure different aspects of the system's reliability and reproducibility. 15. Clearly document and operationalize processes for the testing and verification of the reliability and reproducibility of the AI system. 16. Define tested failsafe fallback plans to address AI system errors of whatever origin and put governance procedures in place to trigger them. 17. Put in place a proper procedure for handling the cases where the AI system yields results with a low confidence score.

Table 2. Technical robustness and safety ethics recommendations

Privacy and Data Governance

Requeriment	Recomendations
Besides ensuring full respect for privacy and data protection, adequate data governance mechanisms must also be ensured, taking into account the quality and integrity of the data, and ensuring legitimised access to data.	1. Take measures to consider the impact of the AI system on the right to privacy, the right to physical, mental and/or moral integrity and the right to data protection. 2. Consider establishing mechanisms that allow flagging issues related to privacy or data protection concerning the AI system. 3. When relevant, implement the right to withdraw consent, the right to object and the right to be forgotten in the AI system. 4. Consider the privacy and data protection implications of data collected, generated or processed over the course of the AI system's lifecycle. 5. Consider the privacy and data protection implications of the AI system's non-personal training-data or other processed non-personal data. 6. Whenever possible and relevant, align the AI-system with relevant standards (e.g. ISO, IEEE) or widely adopted protocols for (daily) data management and governance.

Table 3. Privacy and Data Governance ethics recommendations

Transparency

Requeriment	Recomendations
The data, system and AI business models should be transparent. Traceability mechanisms can help achieving this. Moreover, AI systems and their decisions should be explained in a manner adapted to the stakeholder concerned. Humans need to be aware that they are interacting with an AI system, and must be informed of the system's capabilities and limitations.	1. Consider adopting measures to continuously assess the quality of the input data to the AI system. 2. Consider explaining the decision adopted or suggested by the AI system to its end users. 3. Consider continuously surveying the users to ask them whether they understand the decision(s) of the AI system. 4. In case of interactive AI system, consider communicating to users that they are interacting with a machine.

Table 4. Transparency ethics recommendations

Diversity, non-discrimination and fairness

Requeriment	Recomendations
Unfair bias must be avoided, as it could could have multiple negative implications, from the marginalization of vulnerable groups, to the exacerbation of prejudice and discrimination. Fostering diversity, AI systems should be accessible to all, regardless of any disability, and involve relevant stakeholders throughout their entire life circle.	1. Consider establishing a strategy or a set of procedures to avoid creating or reinforcing unfair bias in the AI system, both regarding the use of input data as well as for the algorithm design. 2. Consider diversity and representativeness of end-users and/or subjects in the data. 3. Test for specific target groups or problematic use cases. 4. Research and use publicly available technical tools, that are state-of-the-art, to improve your understanding of the data, model and performance. 5. Assess and put in place processes to test and monitor for potential biases during the entire lifecycle of the AI system (e.g. biases due to possible limitations stemming from the composition of the used data sets (lack of diversity, non-representativeness). 6. Consider diversity and representativeness of end-users and or subjects in the data. 7. Put in place educational and awareness initiatives to help AI designers and AI developers be more aware of the possible bias they can inject in designing and developing the AI system. 8. Depending on the use case, ensure a mechanism that allows for the flagging of issues related to bias, discrimination or poor performance of the AI system. 9. You should establish clear steps and ways of communicating on how and to whom such issues can be raised. 10. Identify the subjects that could potentially be (in)directly affected by the AI system, in addition to the (end)-users. 11. Your definition of fairness should be commonly used and should be implemented in any phase of the process of setting up the AI system. 12. Consider other definitions of fairness before choosing one. 13. Consult with the impacted communities about the correct definition of fairness, such as representatives of elderly persons or persons with disabilities. 14. Ensure a quantitative analysis or metrics to measure and test the applied definition of fairness. 15. Establish mechanisms to ensure fairness in your AI system. 16. You should ensure that the AI system corresponds to the variety of preferences and abilities in society. 17. You should assess whether the AI system's user interface is usable by those with special needs or disabilities or those at risk of exclusion. 18. You should ensure that Universal Design principles are taken into account during every step of the planning and development process, if applicable. 19. You should take the impact of the AI system on the potential end-users and/or subjects into account. 20. You should assess whether the team involved in building the AI system engaged with the possible target end-users and/or subjects. 21. You should assess whether there could be groups who might be disproportionately affected by the outcomes of the system. 22. You should assess the risk of the possible unfairness of the system onto the end-user's or subject's communities. 23. You should consider a mechanism to include the participation of the widest range of possible stakeholders in the AI system's design and development.

Table 5. Diversity, non-discrimination and fairness ethics recommendations

Societal and environmental well-being

Requeriment	Recomendations
AI systems should benefit all human beings, including future generations. It must hence be ensured that they are sustainable and environmentally friendly. Moreover, they should take into account the environment, including other living beings, and their social and societal impact should be carefully considered.	1. Consider the potential positive and negative impacts of your AI system on the environment and establish mechanisms to evaluate this impact. 2. Define measures to reduce the environmental impact of your AI system's lifecycle and participate in competitions for the development of AI solutions that tackle this problem. 3. Inform and consult with the impacted workers and their representatives but also involve other stakeholders. Implement communication, education, and training at operational and management level. 4. Take measures to ensure that the work impacts of the AI system are well understood on the basis of an analysis of the work processes and the whole socio-technical system. 5. Take measures to counteract de-skilling by means of continuous training, especially in areas sensitive in terms of safety and security. 6. Provide training opportunities and materials for re- and up-skilling measures.

Table 6. Societal and environmental well-being ethics recommendations

Accountability

Requeriment	Recomendations
Mechanisms should be put in place to ensure responsibility and accountability for AI systems and their outcomes. Auditability, which enables the assessment of algorithms, data and design processes plays a key role therein, especially in critical applications. Moreover, adequate an accessible redress should be ensured.	1. Designing a system in a way that can be audited later, results in a more modular and robust system architecture. Thus, it is highly recommended to ensure modularity, traceability of the control and data flow and suitable logging mechanisms. 2. To facilitate 3rd party auditing can contribute to generate trust in the technology and the product itself. Additionally, it is a strong indication of applying due care in the development and adhering to best practices and industrial standards. 3. To foresee 3rd party auditing or guidance can help with both, qualitative and quantitative risk analysis. In addition, it can contribute to generate trust in the technology and the product itself. 4. AI systems should be developed with a preventative approach to risks and in a manner such that they reliably behave as intended while minimising unintentional and unexpected harm, and preventing unacceptable harm. Consequently, developers and deployers should receive appropriate training about the legal framework that applies for the deployed systems. 5. A useful non-technical method to ensure the implementation of trustworthy AI is to include various stakeholders, e.g. assembled in an "ethical review board" to monitor and assist the development process. 6. If AI systems are increasingly used for decision support or for taking decisions themselves, it has to be made sure these systems are fair in their impact on people's lives, that they are in line with values that should not be compromised and able to act accordingly, and that suitable accountability processes can ensure this. Consequently, all conflicts of values, or trade-offs should be well documented and explained. 7. Involving third parties to report on vulnerabilities and risks does help to identify and mitigate potential pitfalls. 8. A risk management process should always include new findings since initial assumptions about the likelihood of occurrence for a specific risk might be faulty and thus, the quantitative risk analysis was not correct and should be revised with the new findings. 9. Acknowledging that redress is needed when incorrect predictions can cause adverse impacts to individuals is key to ensure trust. Particular attention should be paid to vulnerable persons or groups.

Table 7. Accountability ethics recommendations

2.1.3. Secondary ethics issues

It is strongly recommended that SYNERGISE project partners also consider the following specific ethical recommendations, although they are not mandatory, once the key ethical requirements have been identified and explained. These requirements are intended to broaden the scope of the ethical framework developed in this deliverable and to provide greater assurance to project partners.

Incidental findings

According to European Commission, incidental findings are a possible ethical issue that have to be taken into consideration in research projects development. In order to tackle possible incidental findings European Commission has launched several documents such as: Horizon 2020 Programme Guidance How to complete your ethics self-assessment[27], EU Grants How to complete your ethics self-assessment[28], Ethics in Social Science and Humanities[29] in which it is clearly expressed the necessity of define: what procedures will be implemented in the event of unexpected or incidental findings (in particular, how and when participants will be informed about such finding, whether they have the right "not to know" about any such findings, and whether relevant findings (e.g. genetic information) might affect relatives as well)[30].

In this regard, incidental findings can be defined as: results that are outside the original purpose for which a test or procedure was conducted[31]. Incidental findings can also be: Results referring to cases that, based on the knowledge and judgment of the researchers involved in the project, are obviously illegal or potentially critical. For example: abusive practices, illegal data collecting, violation of privacy or violation of ethical codes.

In addition, incidental findings can be either "anticipatable" or "unanticipatable." An anticipatable incidental finding is one that is expected to be associated with a test or procedure. Anticipatable incidental findings need not be common or even likely to occur—their defining characteristic is that the possibility of finding them is known[32]. On the other hand, unanticipatable incidental findings include findings that could not have been anticipated given the current state of scientific knowledge. Researchers cannot plan for these types of findings specifically. However, they can consider in advance what they might do if a particular kind of unexpected finding arises33. There is also possible potential situation in where could it be necessary to deal with secondary finding, these findings are not the primary target of the test or procedure; instead of that, it is an additional result actively sought by the research group. Secondary findings might be searched deliberately when doing so is recommended by an expert body or by a consensus of practitioners. Following the instructions defined by European Commission, researchers have an obligation to address the possibility of discovering incidental findings or secondary findings and describing in advance the procedure that shall be followed in such case acting both proactively (for instance acquiring consent forms by the participants), as well as following such findings (confidentiality, communication to research participants etc[34]. Precisely, related to this, one of the main ethical concerns when incidental findings in research occur is whether or not these findings should be disclosed to the rest of research participants. In this sense, researchers could ask themselves about following questions:

- How should an incidental finding of potential significance be dealing in the research setting?

[27] European Commission (2019). Horizon 2020 Programme Guidance How to complete your ethics self-assessment
[28] European Commission (2021) How to complete your ethics self-assessment. Available at: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/how-to-complete-your-ethics-self-assessment_en.pdf
[29] European Commission (2018). Ethics in Social Science and Humanities. Available at: https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/ethics_en.htm
[30] European Commission (2021) How to complete your ethics self-assessment. p. 9.
[31] European Commision (2019). D 1.6 Incidental Findings Policy, p. 7.
[32] European Commision (2019). D 1.6 Incidental Findings Policy, p. 8.
[33] European Commision (2019), p. 8.
[34] European Commision (2019), p. 7.

- Should it be communicated to the research subject or not?
- Should participant privacy be safeguarded?
- Whose responsibility is it to communicate the incidental finding to a subject, to follow up, and to treat if needed?
- Who shall be responsible to evaluate potential risks and benefits of such disclosure and ultimately take the final decision of whether to communicate such incidental findings or not?[35]

As far as researchers are concerned the main ethical concern that needs to be addressed is: Are researchers ethically obligated to share such information with study participants and, if yes, are they qualified to do so? According to this, transparency and responsibility in the research process should be one of the pillars of the SYNERGISE project enquiry. For this reason, researchers have an ethical duty to notify to the participants, competent authorities or to the responsible organizational position, i.e., law enforcement agencies and/or the management the possible incidental findings. Moreover, based on the recommendations of the Ethics in Social Science and Humanities document, it is recommendable to take into consideration the following:

- Plan ahead by drafting a policy for dealing with unintended, unexpected, or incidental findings that are not harmless.
- Inform participants about the limits of the confidentiality that you can offer (the information sheet should cover incidental findings policy).
- Be aware of the legal context in which you conduct your research and consult your host institution's legal department (see also covert research, above) to ensure that your research design is within legal limits.
- Include in your work plan a structure for discussing unexpected or incidental findings within your consortium[36].

Incidental findings in the context of SYNERGISE

The possibility of incidental findings occurring in the context of the SYNERGIZE project may vary depending on the activities intended to be carried out. However, in order to offer a guide that is as exhaustive and at the same time concrete as possible, this subsection has been prepared in which a series of recommendations are offered that, presumably, should guide the course of action of the researchers involved in the tasks. In first place, incidental findings need to be taken into consideration when researchers design their consent forms. More specifically, researchers should inform potential research participants in the informed consent process and forms that:

- Incidental findings may be found;
- Describe to them the anticipated incidental findings that may arise;
- Inform them of the process by which incidental findings will be evaluated;
- Inform them of the circumstances under which they will be communicated to them, as well as of the disclosing process;
- Indicate how participants might opt out of receiving certain findings;
- Most importantly, researchers should acquire the participants' written and clear consent that they wish such findings, if any, to be notified to them[37].

On the other hand, following the indications of *The Bioethics Commission* in its document on *Anticipate and Communicate Ethical Management of Incidental and Secondary Findings in the Clinical, Research, and Direct-to-Consumer Contexts* there are four ethical principles to be particularly applicable to the ethical assessment of incidental and secondary findings: respect for persons, beneficence, justice and fairness, and intellectual freedom and responsibility. These ethical principles are fundamental to develop proper ethical assessment.

[35] European Commission (2019), p. 8.
[36] European Commission (2019). Ethics in Social Science and Humanities, p.15.
[37] European Commission (2019). Ethics in Social Science and Humanities, p.10.

In parallel of the document of the European Commission, The Bioethics Commission also prescribes some general recommendations which it is highly recommended to take into account. In concrete five recommendations: Informing persons tested, evidence-based practice guidelines, additional empirical research, educating stakeholders and finally, justice and fairness and health inequalities. Those five recommendations given by The Bioethics Commission can be explained as follows

Regarding Informing Persons Tested:

In all contexts, potential recipients of incidental and secondary findings— patients, research participants, and consumers—should be informed about the likelihood of such findings arising from a particular test or procedure. Providing this information enables a potential recipient to make an autonomous decision about whether and how to proceed. Researchers should also clearly communicate to participants the plan for disclosing and managing anticipatable incidental findings as well as any possible secondary findings, and the distinction between research and clinical care. This communication is essential to ensure that participants understand what to expect as a result of their decision to participate in research. Clarity with respect to whether and how researchers will disclose anticipatable and unanticipatable incidental findings, and any secondary findings that are deliberately sought, can help sustain public and participant trust in the research enterprise[38].

Regarding Evidence-Based Practice Guidelines:

Practice guidelines can inform practitioners about the anticipatable incidental findings likely to arise during common tests and procedures, and the ways in which practitioners can best manage these findings—including the possibility of actively seeking particular findings as secondary findings[39].

Regarding Additional Empirical Research:

Additional empirical research and scholarship is needed concerning the discovery, disclosure, and management of incidental and secondary findings[40].

Regarding Educating Stakeholders:

Educating the public about incidental and secondary findings enables those undergoing tests or procedures to make better informed decisions and develop informed preferences about receiving potential findings. Educating practitioners about their ethical obligations enables them to make more s thoughtful decisions about how to anticipate, disclose, and manage incidental and secondary findings[41]

Regarding Justice and Fairness and Health Inequities

Justice and fairness in health care requires that all individuals have access to adequate affordable services to meet basic health care needs.

Moreover, in order to provide some more context-specific guidance to FRs the following recommendations are given:

Recommendation 1:

Clinicians, researchers, and direct-to-consumer providers should describe to potential recipients incidental and secondary findings that are likely to arise or be sought from the tests and procedures conducted. Practitioners should inform potential recipients about their plan for disclosing and managing incidental and secondary findings, including what findings will and will not be returned[42].

Recommendation 2:

[38] Presidential Commission for the Study of Bioethical Issues (2013). Anticipate and Communicate Ethical Management of Incidental and Secondary Findings in the Clinical, Research, and Direct-to-Consumer Contexts, p.14
[39] Presidential Commission for the Study of Bioethical Issues (2013), p.6
[40] Presidential Commission for the Study of Bioethical Issues (2013), p.7
[41] Presidential Commission for the Study of Bioethical Issues (2013), pp.7-8
[42] Presidential Commission for the Study of Bioethical Issues (2013), p.5.

Professional representative groups should develop guidelines that categorize the findings likely to arise from each diagnostic modality; develop best practices for managing incidental and secondary findings; and share these guidelines among practitioners in the clinical, research, and direct-to consumer contexts[43]

Recommendation 3:
Public and private entities should prepare educational materials to inform all stakeholders—including practitioners, institutional review boards, and potential recipients—about the ethical, practical, and legal considerations raised by incidental and secondary findings[44].

Recommendation 4:
The principle of justice and fairness requires that all individuals have access to adequate information, guidance, and support in making informed choices about what medical tests to undergo, what kind of information to seek, and what to do with information once received. The principle of justice and fairness also requires affordable access to quality information about incidental and secondary findings, before and after testing, which when coupled with access to care can be potentially lifesaving or life enhancing[45].

Recommendation 5:
During the informed consent process, researchers should convey to participants the scope of potential incidental or secondary findings, whether such findings will be disclosed, the process for disclosing these findings, and whether and how participants might opt out of receiving certain types of findings[46].

Recommendation 6:
Researchers should develop a plan to manage anticipatable incidental findings, including but not limited to those findings known to be significant and clinically actionable (and, when relevant, analytically valid and clinically valid). The plan should be reviewed and approved by an institutional review board[47].

Recommendation 7:
Researchers should develop a process for evaluating and managing unanticipatable findings. The plan should be reviewed and approved by an institutional review board. During the informed consent process, researchers should notify participants about the possibility of unanticipatable incidental findings, including lifesaving incidental findings, and the plan for their management. Researchers who discover an unanticipatable incidental finding of concern should assess its significance, consulting with experts as appropriate[48].

Recommendation 8:
Researchers should consider carefully the decision to actively look for secondary findings. In certain circumstances, with approval from an institutional review board, researchers can justifiably adopt a plan that includes looking for selected clinically significant and actionable secondary findings. Approved plans should be disclosed to prospective participants during the informed consent process[49].

Integrity of research practices

Good practices in the context of research and innovation are essential to ensure the smooth running of the projects that are planned to be carried out. These practices guide and assist the

[43]Presidential Commission for the Study of Bioethical Issues (2013), p.6.
[44] Presidential Commission for the Study of Bioethical Issues (2013), p.8.
[45] Presidential Commission for the Study of Bioethical Issues (2013), p.9.
[46]Presidential Commission for the Study of Bioethical Issues (2013), p.14.
[47] Presidential Commission for the Study of Bioethical Issues (2013), p.15.
[48] Presidential Commission for the Study of Bioethical Issues (2013), p.15.
[49] Presidential Commission for the Study of Bioethical Issues (2013), p.16

different participants involved in the research work throughout the project and allow them to be aware of the ethical and practical challenges that the development of their work may entail. In this sense, if we take as a reference the document *The European Code of Conduct for Research Integrity*, the following can be highlighted:

- Reliability in ensuring the quality of research, reflected in the design, methodology, analysis, and use of resources.
- Honesty in developing, undertaking, reviewing, reporting, and communicating research in a transparent, fair, full, and unbiased way.
- Respect for colleagues, research participants, research subjects, 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 for its wider societal impacts50.

According to the previous cited document, research misconduct is traditionally defined as fabrication, falsification, or plagiarism (the so-called FFP categorisation) in proposing, performing, or reviewing research, or in reporting research results:

- Fabrication is making up data or results and recording them as if they were real.
- Falsification is manipulating research materials, equipment, images, or processes, or changing, omitting, or suppressing data or results without justification.
- Plagiarism is using other people's work or ideas without giving proper credit to the original source51

Ethical impact assessment

According to European Commission, Ethics Assessment is an in-depth analysis of the ethical issues of the proposals, considering, when available the conclusions of the Ethics screening[52]. Also, according to SATORI project[53] the function of the ethical impact identification stage can be explained like this:

- Describe possible and probable futures regarding the ethical impacts of the R&I project.
- Describe the relevant research outcomes that can lead to ethical impacts.
- Identify ethical values and principles and relevant stakeholder interests regarding these impacts.

In this sense, it is strongly recommended that the consortium members establish different ethical review groups to assess the ethical impact implications of the whole process carried out during the project. Moreover, the following considerations may offer a perspective on the issue[54]:

- Has the ethical assessment been a part of the elaboration and implementation process of development and deployment of this project?
- Have different stakeholders been taken into consideration to carry out the research?
- Is a periodic ethics review foreseen?

2.2. Privacy issues of SYNERGISE

The European Commission has always been concerned to ensure that the fundamental rights it recognises for Union citizens are respected and this means adapting to new challenges that may arise in society. In recent years, one of these challenges is represented by the rapid development

[50] ALLEA (2023). The European Code of Conduct for Research Integrity -Revised Edition 2023,.p.5 Available at: https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/ethics_en.htm
[51] ALLEA (2023). The European Code of Conduct for Research Integrity -Revised Edition 2023,.p10.Available at: https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/ethics_en.htm
[52] Available at: https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/ethics_en.htm Last seen (20/01/2024)
[53] This project was dedicated to develop a common European Framework for ethical assessment of research and innovation. For more information: https://satoriproject.eu/ Last seen (20/01/2024)
[54] This list of considerations is non-exhaustive.

of new technologies, where the volume of data collected and exchanged has grown exponentially and economic and social integration has also led to a substantial increase in cross-border data flows. Citizens themselves make more and more personal data available to the public without really knowing the consequences that may arise from it. With this in mind, for the European Commission, data protection has become both a central issue for research ethics in Europe and a fundamental human right.

As a fundamental right, data protection is intimately linked to autonomy and human dignity and to the principle that everyone should be valued and respected. It is enshrined in the EU Charter of Fundamental Rights and the Treaty on the Functioning of the European Union, which give effect to individuals' right to privacy by providing them with control over the way information about them is collected and used. On the other hand, as central issue in research projects, data protection imposes obligations on researchers to provide research participants with detailed information about what happen to the personal data that they collect. It also requires the organisations processing the data to ensure the data are properly protected, minimised, and destroyed when no longer needed.

Legal frameworks of EU and the Council of Europe that safeguard the protection of privacy and personal data have recently been reviewed, placing Europe legislation at the forefront of data protection worldwide. The EU's data protection standards are based on Council of Europe Convention 108, EU instruments – including the General Data Protection Regulation and the Data Protection Directive for Police and Criminal Justice Authorities – as well as on the respective case law of the European Court of Human Rights and of the Court of Justice of the European Union.

The data protection reforms carried out by the EU and the Council of Europe are extensive and at times complex, with wide-ranging benefits and impact on individuals and businesses. Due to this, the present handbook aims to raise awareness and improve knowledge of data protection rules, especially among non-specialist legal practitioners who have to deal with data protection issues in SYNERGISE project.

2.1.1. General Privacy Issues

SYNERGISE activities will collect and treat personal data, so the main characteristics of data protection regulation and some other aspects related to personal data is analysed in this section.

Personal Data notion

The current European Union legislation defines *personal data* as any information relating to a natural person who can be identified directly from the information in question, or indirectly from that information in combination with other information[55]. To determine whether a person is identifiable, a controller or another person must consider all reasonable means that are likely to be used to directly or indirectly identify the individual. Furthermore, direct or indirect identifiability of individuals requires continuous assessment, 'taking into consideration the available technology at the time of the processing and technology developments '.[56] If data about such a person are being processed, this person is called the 'data subject'. Under European Union law, natural persons are the only beneficiaries of data protection rules, so such regulation does not cover data processing which concern legal persons – in particular does not concern undertakings established as legal persons, including the name and form of the legal person and their contact details[57] – . However,

[55]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, Art. 4 (1).
[56]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, Recital 26.
[57]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, Recital 14.

the e-Privacy Directive protects the confidentiality of communications and the legitimate interests of legal persons concerning the increasing capacity for the automated storage and processing of data relating to subscribers and users[58].

Personal data covers information pertaining to the private life of a person, which also includes professional activities, as well as information about his or her public life. A name and surname; a home address; an email address such as name.surname@company.com; an identification card number; location data; an Internet Protocol (IP) address; a cookie ID; the advertising identifier of your phone; someone's voice; or data held by a hospital which could be a symbol that uniquely identifies a person are some examples of personal data. Quite the opposite, a company registration number; an email address such as info@company.com; information about a deceased person; or anonymised data are not considered personal data.

Personal data also includes *sensitive data*, a special category of personal data which, by their nature, may pose a risk to the data subjects when processed and need enhanced protection. Such data are defined as data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation[59]. Sensitive data also includes criminal conviction and offences data which processing may only be carried out "under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects"[60].
The main difference between both categories of personal data just refers to the conditions for their processing and such processing is defined as "any operation [...] 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 of personal data"[61].

The General Data Protection Regulation (GDPR) and National Regulations

The regulations to which SYNERGISE is directly subject during the execution of the research activities are:

- 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 movement of such data, and repealing the Directive 95/46/EC (General Data Protection Regulation)
- National regulation to which each SYNERGISE partner

The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world which imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. Its primary aim is to give individuals control over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. In this way, the regulation is an essential step to strengthen individuals' fundamental rights in the digital age and facilitate business by clarifying rules for companies and public bodies in the digital single market.

[58]Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Recital 7 and Art. 1 (2).
[59] 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, Art. 9.
[60]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, Art. 10.
[61]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, Art. 4 (2).

The GDPR is composed of 99 articles divided in 11 chapters in which general provisions, data subject's rights, controller and processor's obligations, principles and requirements relating to processing of personal data, as well as penalties are established. The following are some of the chapters and articles that have the greatest potential impact in SYNERGISE:

- Article 7 establishes the conditions that informed consent has to accomplish.
- Article 31 specifies requirements for single data breaches: controllers must notify Supervising Authorities of a personal data breach within 72 hours of learning of the breach and must provide specific details of the breach such as the nature of it and the approximate number of data subjects affected.
- Article 32 requires data controllers to notify data subjects as quickly as possible of breaches when the breaches place their rights and freedoms at high risk.
- Articles 33 and 33a require data controllers to perform Data Protection Impact Assessments (DPIA) to identify risks to consumer data and Data Protection Compliance Reviews to ensure those risks are addressed.
- Article 35 requires that certain data controllers appoint data protection officers. Specifically, any company that processes data revealing a subject's genetic data, health, racial or ethnic origin, religious beliefs, etc. must designate a data protection officer; these officers serve to advise data controllers about compliance with the regulation and act as a point of contact with SAs. Some data controllers may be subjected to this aspect of the GDPR simply because they collect personal information about their employees as part of human resources processes.
- Articles 36 and 37 outline the data protection officer position and its responsibilities in ensuring GDPR compliance as well as reporting to Supervisory Authorities and data subjects.

Also, the national legislation in force in the specific country where the processing is being conducted must be respected. This is especially relevant when national regulations are more stringent or impose a greater number of requirements. In the case of a double EU-national regulation, it is always necessary to consider the one that is more protective for the individuals concerned. However, in the EU states most legal national instruments on data protection are a transcript of the GDPR, so there may be not big differences.

2.1.2. High-risk processing indicators

SYNERGISE's high commitment to the highest standards of compliance in the field of personal data protection is expressed through the application of the principle of "minimum risk". This concept is used to denote research in which the probability and magnitude of expected harm or discomfort is not greater than that usually encountered in everyday life or during routine physical or psychological examinations or tests. In relation to this, one of the core obligations in the GDPR is that of the security of personal data which covers confidentiality, integrity and availability and which should be considered following a risk-based approach: the higher the risk (for the rights and freedoms of data subjects), the more rigorous the measures that the controller or the processor needs to take (in order to manage the risk)[62]. Due to this, in November 2018, the European Commission promulgated some instructions on "Ethics and Data Protection" to underline what aspects from a project may entail higher privacy risks. According to such document a project raises higher data privacy risks if it involves:

A. The processing of special categories of personal data (formerly known as *sensitive data*).

[62] In particular, the security of personal data processing is mainly mandated in 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, Article 32.

B. The processing of personal data concerning children, vulnerable people or people who have not given their consent to participate in the research. For SYNERGISE activities, parental consent is always required for children under 18 or incapable of giving informed consent.
C. Complex data processing operations: large scale processing of personal data systematic monitoring of a publicly accessible area on a large-scale involvement of multiple datasets and/or service providers, or the combination and analysis of different datasets (i.e. big data).
D. The use of data processing techniques that are invasive and deemed to pose a risk to the rights and freedoms of research participants, or the use of techniques that are vulnerable to misuse. The covert observation, surveillance, tracking or deception of individuals; using camera systems to monitor behaviour or record sensitive information data mining (including data collected from social media networks); web crawling or social network analysis profiling individuals or groups (particularly behavioural or psychological profiling); or using artificial intelligence to analyse personal data using automated decision making that has a significant impact on the data subject(s), are some examples of these type of techniques.
E. The collection of data outside the EU or the transfer of personal data collected in the EU to entities in non-EU countries.
F. The use of previously collected data (what is also known as secondary data).

If the activities of a project are likely to entail a high-risk for data subjects' privacy, a Data Protection Impact Assessment (DPIA) is required by European law[63]. The DPIA is a preventive tool that must be carried out by the controller to identify, assess, and manage the risks to which its processing activities are exposed with the aim of guaranteeing the rights and freedoms of natural persons. It makes possible to establish the most appropriate control measures to reduce the risks of data processing to a level that is considered acceptable. SELP+I Impact Assessment (D8.2) will be submitted in M42.

2.1.3. SYNERGISE Data Protection Policy

For SYNERGISE activities that intend to implement any processing of personal data, the following shall be complied with:

#	ACTION	RESPONSIBLE	RECEIVER	DEADLINE
1	Submission of a document establishing an identification of all types of data to be processed in the activity (e.g. pulse rate, blood oxygen level, names, etc.) and a justification of the processing in relation to the purposes of the activity.	Task leader	PLUSETHICS	2 months before the start of the activity
2	Submission of: A) Data flow scheme: which organisation will collect and who will have access to the raw data; B) What method of pseudonymisation or anonymisation will be carried out; C) How the raw and pseudo/anonymised data will be stored.	Task leader	PLUSETHICS	1 month before the start of the activity
3	Adaptation of the information and informed consent sheet template.	Task leader	PLUSETHICS	2 weeks before the start of the activity

Table 8. *SYNERGISE Data Protection Policy*

If a transfer of personal data between EU and non-EU partners is envisaged, the need for the signature of a Data Sharing Agreement between the parties will be considered. Whenever personal data are directly collected from research participants, their informed consent must be seek by a procedure that meets the minimum standards of the GDPR. Informed consent requires to explain to data subjects what type of personal data is going to be collected; why that information is needed; how it is going to be processed; what their participation in the project entails; any risks that may be involved; and information about the rights and guarantees that they have. Only after this consent had been given, the personal data could be treated[64]. This requires consent to be given by a clear

[63]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, Article 35.
[64] Informed consent is regulated in 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, Articles 4(11) and 7.

affirmative act establishing a freely given, specific, informed, and unambiguous indication of the subject's agreement to the processing of their personal data[65]. Therefore, the data subject must be provided with detailed information about the envisaged data processing in an intelligible and easily accessible form, using clear and plain language. As a minimum, this should include:

- The identity of the data controller and, where applicable, the contact details of the DPO.
- The specific purpose(s) of the processing for which the personal data will be used.
- The subject's rights as guaranteed by the GDPR and the EU Charter of Fundamental Rights, in particular the right to withdraw consent or access their data, the procedures to follow should they wish to do so, and the right to lodge a complaint with a supervisory authority.
- Information as to whether data will be shared with or transferred to third parties and for what purposes.
- How long the data will be retained before they are destroyed.

The data subjects must also be made aware if data are to be used for any other purposes, shared with research partners or transferred to organisations outside the EU[66].

SYNERGISE has a general information sheet and informed consent template (see Annex 1).

[65]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, Article 6.
[66]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, Article 13.

3. Ethics & Privacy Governance

3.1. Ethical decision processes

Ethical decision making is a critical component of any organisation's operations. These decisions not only reflect the values and integrity of the organisation, but also have a significant impact on trust and reputation in the marketplace. In the context of privacy and ethics governance, ethical decisions ensure that the organisation not only complies with laws and regulations, but also respects the rights and expectations of all stakeholders. Establishing a clear and well-defined process for ethical decision-making is essential to maintain consistency, transparency, and accountability throughout the organisation's operations. This involves careful consideration of how actions and policies affect both internal individuals and society at large and ensures that ethical values are at the heart of all R+D decisions.

3.1.1. Ethical decision-making process

This process is articulated in three fundamental stages: 1) identification of ethical dilemmas, 2) analysis and deliberation, and 3) decision making and justification. Each of these stages plays a critical role in ensuring that the decisions made are ethically sound and consistent with the SYNERGISE's values and principles. On the other hand, this ethical decision-making process is dynamic and requires constant review and updating to adapt to new ethical challenges and changes in the project environment.

1. Identifying ethical issues:
   - This stage is the starting point of the ethical decision-making process. It involves recognising situations that present moral conflicts.
   - Partners must be trained to identify these issues, which requires a thorough understanding of the organisation's values and ethical principles.
   - Tools such as codes of ethics, training and what-if scenarios could be used to enhance the ability to identify ethical dilemmas.

2. Analysis and deliberation:
   - In this stage, identified ethical issues are analysed by considering different perspectives and possible outcomes.
   - Methods such as stakeholder analysis, ethical impact assessment and structured ethical debates could be used to explore the implications of decisions from different perspectives.
   - This stage also involves considering ethical alternatives, assessing the pros and cons of each option and their consistency with the organisation's values.

3. Decision making and justification:
   - This is the final stage where an informed ethical decision is made and properly justified.
   - The decision must be consistent with the values and ethical principles of the project and consider the results of the analysis and deliberation.
   - Justification of decisions is essential to ensure transparency and accountability. This includes documenting the decision-making process and the reasons for the choice made.

3.1.2. Roles and responsibilities

At SYNERGISE, the structure of roles and responsibilities for ethical decision-making is fundamental to ensuring the effectiveness and coherence of this process. SYNERGISE has established a clear and functional hierarchy with several levels and specific roles. This structure ensures that ethical decision-making is an integrated and coherent process at all levels of SYNERGISE, reinforcing the ethical culture and shared responsibility throughout the project.

1) Coordination (THW):
   - They promote the ethical values of the project.
   - They are responsible for making high-level ethical decisions and establishing ethical policies and procedures.

2) Ethics and legal experts (PLUSETHICS):
   - They play a crucial role in reviewing and discussing complex ethical dilemmas.
   - They facilitate ethical decision making and ensure alignment with SYNERGISE´s values.
   - They are responsible for monitoring compliance with ethics policies and are the point of contact for ethics-related issues.
   - They provide guidance and support for ethical decision-making at the operational level.

3) Consortium Partners
   - Responsible for identifying and reporting ethical dilemmas.
   - They must adhere to ethical values in their day-to-day decision-making.

3.1.3. Ethical awareness and training

Ethics training and awareness are of paramount importance in the context of European security projects such as SYNERGISE. A thorough understanding and effective management of ethical and privacy issues is essential in a sector where decisions can have significant national and international consequences. These projects must comply not only with strict legal and regulatory standards, but also with high ethical principles that ensure trust and legitimacy in the defense and security sector. Therefore, a sound ethical background is essential to ensure that all project actions and decisions are in line with these high ethical and legal standards. In the SYNERGISE project, the training and ethical awareness section focuses on two main activities: 1) a webinar on identifying and managing ethical and privacy issues in the context of European defense funds and 2) sessions on promoting the management of ethical and privacy issues at each coordination meeting. These activities are designed to promote a thorough understanding and effective management of the ethical and privacy issues that are critical to the success of the SYNERGISE project.

1. Webinar on the identification and management of ethical and privacy issues in the context of European defense funds (available at SYNERGISE shared point):
   - This webinar focused on understanding and managing specific ethical and privacy issues in the context of Horizon Europe Funds.
   - It covered topics such as identifying potential ethical dilemmas, applying relevant data protection legislation and best practices for dealing with these issues in the project context.
   - The webinar included expert presentations, Q&A sessions, and case studies to illustrate practical situations.

2. Sessions to promote the management of ethics and privacy issues at each coordination meeting:
   - During the regular coordination meetings, a timeslot is dedicated to discussing progress and challenges in managing the ethical and privacy aspects of the project.
   - These meetings allow for a continuous exchange of experiences, lessons learned and best practices among team members.

The active participation of all members is encouraged to share their observations and proposed solutions to ethical and privacy challenges that arise.

3.2. Updates and reviews

This section of the SYNERGISE Ethics and Privacy Handbook is an essential part of maintaining the relevance and effectiveness of the Ethics and Privacy Policy over time. This process ensures that the Handbook is kept up to date not only with the latest legal and regulatory developments, but also with technological advances and changing societal expectations. Furthermore, this process of updating and reviewing is essential for SYNERGISE to maintain a high standard of ethics and privacy in a rapidly changing environment and to ensure that its practices and policies remain relevant, effective and accountable.

- Periodic review process: the Handbook should be reviewed periodically, preferably annually, to ensure that it remains current with new laws, regulations and best practices in ethics and privacy.
- Stakeholder involvement: it is important to involve a variety of stakeholders in the review process, including partners, legal and ethical experts, and ad hoc committees established to oversee the project. This will ensure a diverse and comprehensive perspective.
- Feedback and suggestions: a system where partners and other stakeholders can provide feedback and suggestions on the content of the handbook is encouraged. This could be done through specific meetings, focus groups or internal communication channels. Based on the review and feedback, updates should be made to the handbook. This will include modifying existing policies and adding new sections as necessary.
- Assess the impact of technological and social changes: as SYNERGISE operates in a highly technological and dynamic sector, it is crucial to assess how technological developments and changes in the social environment affect ethical and privacy issues. This will mainly be done in WP8.
- Communication and training on updates: after each update, it is important to communicate the changes to all SYNERGISE partners and to provide additional training and awareness raising if the changes are substantial.
- Documentation and change log: maintain a detailed record of all changes made to the manual to ensure transparency and facilitate future revisions.

ANNEX

Participant information sheet template (to be adapted)

WORK PACKAGE: [WP NUMBER AND TITLE]
ACTIVITY: [TITLE]
PARTNER LEADING ACTIVITY AND COLLECTING CONSENT: [ORGANIZATION REFERENCE]
You are about to take part in a research activity for the PROJECT EU Horizon Europe project. PROJECT is coordinated by [COORDINATOR] (Country).

Project description
PROJECT's main objective is [DESCRIPTION]

Why have I been approached?
[DESCRIPTION OF THE SELECTED PARTICIPANT PROFILE]

Right to withdraw and to data protection
You do not have to take part in this research if you do not want to. Likewise, you may change your mind about your participation later on and withdraw after taking part in [STUDY/ACTIVITY], without needing to provide a reason. In this case, your input will be securely deleted from our records and servers.
If you wish to withdraw, ask questions or make use of your data protection rights (access, rectification, deletion, information, limitation and portability), you may contact the Data Protection Responsible for this project: [NAME], email [EMAIL]

What will I be asked to do if I take part in this research activity?
If you decide to take part, you will be asked to [DESCRIPTION]
When contributing to [ACTIVITY] with your expertise you may want to share real-life experiences or cases you are or have worked on. Please be aware that this is sensitive information, and you should do your best to not share personal details of anyone involved in any radicalisation process. General details can and should be shared, but those involved must be protected. If you happen to mention specific people, their names will be deleted from any project materials.

Will my data be Identifiable?
When providing your opinions, only your answers will be recorded, and this information will only be processed by project partners, held on the personal, and protected, computer drive of the researcher, and kept separate from the interview material. Therefore, your opinions will not be linked to your name or any other direct identifiers, and opinions that may identify you will not be made public in any case. Any security sensitive information will also be discarded for publication.
Additionally, researchers use secure network servers to exchange information between project partners, and any e-mails inviting experts or discussing the research with participants will be deleted after the research is compiled into the relevant reports.

Any data labelled as personal data (containing your [DETAIL: i.e. name, address, sex, age, etc]) will be deleted 5 years after the end of the project ([YEAR]).

Audio recordings [DELETE IF NOT RELEVANT]
Audio of the session/s which you will participate will be recorded. They will be deleted once the transcripts and/or project reports have been completed. Transcripts will eliminate any information that would enable you to be identified (names, locations, etc.) directly, by inference or by

association. This anonymisation will be complete and irreversible as the original audios will be destroyed.

Video [DELETE IF NOT RELEVANT]

Videos of the session/s which you will participate will be recorded. You can opt-out of video recording by stating it in the consent form. If you agree to video recording, your image and opinions may be used in project materials and dissemination activities, but not reused for research purposes.

What will happen to the results?

The research results will be confidential and only accessible to other project partners and the EU Commission Services. However, project partners may use project results in specialised publications. In no case will these materials include information that could identify you or your opinions. Anonymised direct quotations from your contributions may be used in these reports and publications, but your name or other directly-identifying information will not be included.

What are the risks and benefits of my participation?

Your expertise and knowledge may benefit [DESCRIPTION]

Before starting, you should know that your participation may entail the following risks: [DESCRIPTION]

Who is responsible for the research?

The project has been funded by the EU Horizon Europe and is coordinated by [COORDINATOR] (WEBSITE)file:///C:/Users/flavi/Mi unidad/PROYECTOS EUROPEOS/SYMSITES/(https:/www.aitex.es/). The [PROJECT / DEPARTMENT RESPONSIBLE POSITION] is [NAME] [EMAIL]. Further information on the project can be found on [PROJECT WEBSITE].

Thank you for taking the time to read this information sheet. You can keep this document.

Consent form template (to be adapted)

WORK PACKAGE: [WP NUMBER AND TITLE]
ACTIVITY: [TITLE]
PARTNER LEADING ACTIVITY AND COLLECTING CONSENT: [ORGANIZATION REFERENCE]
RESPONSIBLE: [NAME AND EMAIL]

I hereby confirm that	YES	NO
I have been informed of the project aims and goals		
I have been provided with an Information Sheet		
I consent to my participation in the research		
I understand that I have the right to withdraw from the research at any time without providing a reason		
I understand that I should not share personal details of persons involved in real cases/ processes		
I understand that my personal data will be deleted after the completion of the project		
I consent to my data being used in the future for research purposes only		
I consent to the voice recording of my contributions in the research		
I consent to the video recording of my participation in the research		
I consent to my voice recording being published in [WEB AND PROFILE]		
I consent to my video recording being published in [WEB AND PROFILE]		
I have been provided with the contact details of the responsible of this activity		
I have been provided with the contact details of the project coordinator		

Name:_____

Signature:

Thank you for taking the time to complete this consent form. Please return it to the project research.

Ethics and privacy protocol for human participation research activities

This Ethics and Privacy Protocol has been developed for partners responsible for implementing pilots based on the content of D8.1. It serves as a guidance document outlining the key ethical and privacy considerations to be taken into account before, during and after the implementation of each of the SYNERGISE pilots. This protocol is intended to be a guide to best practice, offering recommendations rather than strict guidelines.

It aims to ensure that all pilot activities are conducted with the highest ethical standards, focusing on areas such as risk and benefit assessment, informed consent and inclusive practices (such as ensuring non-discrimination and promoting diversity). It addresses key issues such as respect for the privacy of participants. It also aligns with the requirements of the GDPR, emphasizing the importance of lawful data processing, data security and respecting the rights of data subjects.

By following this protocol, project partners can ensure ethical integrity, transparency and compliance with legal standards, ultimately contributing to the success of the testing pilots and the societal benefits of SYNERGISE.

Ethics protocol

Protocol stage	Description	Implementation recommendations	Implementation timing
Risk and Benefit Assessment	Conduct a thorough assessment of risks and benefits, adjusting strategies to minimize risks (physical, psychological, economical, reputational, etc.) and maximize benefits for participants and the community.	Develop a comprehensive risk management plan; use tools like SWOT analysis; involve stakeholders in risk assessment.	Before starting the pilot
Informed Consent	Obtain explicit, informed, and voluntary consent from all participants, ensuring their understanding of the project, its risks, and benefits.	Use plain language in consent forms; conduct informational sessions; provide Q&A opportunities for participants.	Before and at the start of the pilot
Confidentiality and Privacy	Implement robust measures to protect the confidentiality and privacy of the collected data, ensuring respect for individual privacy.	Utilize encryption and secure data storage; conduct staff training on privacy policies; regularly update security measures.	Before and during the pilot
Personal Data Protection	Ensure data processing complies with current regulations, including GDPR, respecting individuals' rights over their data.	Stay updated with data protection laws; implement data minimization and purpose limitation principles.	Before and during the pilot
Special Considerations for Minor Participation (if applicable)	Implement additional safeguards when involving minors, such as obtaining consent from parents or guardians, tailoring communication to be age-appropriate, and ensuring an environment that respects minors' unique needs and vulnerabilities.	Establish clear guidelines for minor participation; involve child psychologists in protocol design; ensure legal compliance for minor consent.	Before and throughout the pilot
Non-discrimination and Respect for Diversity	Promote inclusion and diversity in participant selection, avoiding any form of discrimination.	Develop a participant selection framework that emphasizes diversity; conduct unconscious bias training for staff.	During participant selection
Inclusion of Gender and Diversity Policies	Actively integrate gender and diversity policies in all phases of the project to ensure equitable and representative participation.	Include diverse team members in project planning; regularly review and update diversity policies.	When designing and executing the pilot
Safety and Well-being of Participants	Prioritize the safety and well-being of participants through constant risk assessments and adequate emergency protocols.	Implement and regularly review safety protocols; establish a rapid response team for emergencies.	Throughout the pilot
Respect for Human Dignity	Maintain respectful and fair treatment of all participants, safeguarding their dignity at all times.	Provide sensitivity training to staff; establish clear ethical guidelines and a complaint resolution process.	During all interactions
Transparency and Open Communication	Maintain transparent and open communication with participants and other stakeholders, sharing relevant information in a timely manner.	Develop a communication plan that includes regular updates; use multiple channels to reach different audiences.	During and after the pilot
Honesty and Transparency in Research	Maintain integrity in research, ensuring accuracy in data collection and transparency in its presentation and analysis.	Conduct regular internal audits; promote a culture of honesty in research; publish results in accessible formats.	During and after the pilot
Sharing Benefits with Disadvantaged Populations	Identify and collaborate with local communities to ensure that the benefits of the project are shared equitably, especially with disadvantaged populations.	Engage with community leaders; develop programs that address specific community needs; monitor long-term impacts.	After the pilot

Table 9. Ethics protocol summary for human participation activities

Personal data protection protocol[67]

Protocol stage	Description	Implementation recommendations	Implementation timing
Lawful Basis for Processing	Identify and document the legal grounds for data processing before collecting data, such as consent or legitimate interest.	Review legal bases under GDPR; document the justification for each type of data processing; ensure alignment with data protection laws.	Before data collection
Data Minimization	Develop a strategy to collect only essential data, avoiding unnecessary accumulation, aligned with specific purposes.	Create data collection guidelines; regularly review data needs; implement data pruning processes.	Before data collection
Consent Management	Establish a system to obtain, record, and manage clear consent, with provisions for withdrawal.	Develop a user-friendly consent mechanism; maintain an audit trail for consents; implement a straightforward withdrawal process.	Before and at data collection
Data Protection Impact Assessment (DPIA)	Conduct DPIAs for high-risk activities to assess and mitigate data handling risks.	Integrate DPIA into the project planning phase; update DPIAs regularly; involve data protection experts.	As required
Data Security	Implement comprehensive security measures, including anonymization (or pseudonymization) and access controls, to safeguard data.	Apply strong encryption standards; conduct regular security audits; ensure access control protocols.	Before and during data processing
Data Processing Records	Maintain detailed records of processing activities, including data nature, purposes, and security measures.	Use automated tools for record-keeping; ensure clarity and accuracy in documentation; regularly update records.	During data processing
Data Subject Rights	Ensure procedures to respect data subjects' rights, including access, rectification, and erasure.	Implement clear procedures for data subject requests; train staff in handling such requests; regularly review compliance.	Throughout the pilot
Training and Awareness	Provide ongoing GDPR training to staff involved in data processing.	Develop a comprehensive training program; update training materials regularly; ensure staff understanding and compliance.	Ongoing
Data Breach Response Plan	Develop a response plan for data breaches, including immediate actions and notification strategies.	Establish clear procedures for breach detection and response; conduct regular drills; update plan based on emerging threats.	Ongoing
Data Transfer Regulations	Verify GDPR compliance for data transfers outside the EU, ensuring equivalent protection.	Conduct thorough assessments of data transfer channels; ensure contractual and technical safeguards are in place.	As needed
Data Protection Officer (DPO)	Appoint a DPO to oversee GDPR compliance and act as a contact point for authorities, if required.	Select a qualified DPO; ensure they have resources and authority; integrate the DPO in all data protection matters.	As required
Regular Compliance Reviews	Regularly update data protection practices to adapt to new regulations or changes in activities.	Schedule periodic reviews; stay informed about legal changes; involve stakeholders in review processes.	Ongoing
PROTOCOL STAGE	DESCRIPTION	IMPLEMENTATION RECOMMENDATIONS	IMPLEMENTATION TIMING
Lawful Basis for Processing	Identify and document the legal grounds for data processing before collecting data, such as consent or legitimate interest.	Review legal bases under GDPR; document the justification for each type of data processing; ensure alignment with data protection laws.	Before data collection
Data Minimization	Develop a strategy to collect only essential data, avoiding unnecessary accumulation, aligned with specific purposes.	Create data collection guidelines; regularly review data needs; implement data pruning processes.	Before data collection
Consent Management	Establish a system to obtain, record, and manage clear consent, with provisions for withdrawal.	Develop a user-friendly consent mechanism; maintain an audit trail for consents; implement a straightforward withdrawal process.	Before and at data collection
Data Protection Impact Assessment (DPIA)	Conduct DPIAs for high-risk activities to assess and mitigate data handling risks.	Integrate DPIA into the project planning phase; update DPIAs regularly; involve data protection experts.	As required
Data Security	Implement comprehensive security measures, including anonymization (or pseudonymization) and access controls, to safeguard data.	Apply strong encryption standards; conduct regular security audits; ensure access control protocols.	Before and during data processing
Data Processing Records	Maintain detailed records of processing activities, including data nature, purposes, and security measures.	Use automated tools for record-keeping; ensure clarity and accuracy in documentation; regularly update records.	During data processing
Data Subject Rights	Ensure procedures to respect data subjects' rights, including access, rectification, and erasure.	Implement clear procedures for data subject requests; train staff in handling such requests; regularly review compliance.	Throughout the pilot
Training and Awareness	Provide ongoing GDPR training to staff involved in data processing.	Develop a comprehensive training program; update training materials regularly; ensure staff understanding and compliance.	Ongoing
Data Breach Response Plan	Develop a response plan for data breaches, including immediate actions and notification strategies.	Establish clear procedures for breach detection and response; conduct regular drills; update plan based on emerging threats.	Ongoing
Data Transfer Regulations	Verify GDPR compliance for data transfers outside the EU, ensuring equivalent protection.	Conduct thorough assessments of data transfer channels; ensure contractual and technical safeguards are in place.	As needed
Data Protection Officer (DPO)	Appoint a DPO to oversee GDPR compliance and act as a contact point for authorities, if required.	Select a qualified DPO; ensure they have resources and authority; integrate the DPO in all data protection matters.	As required
Regular Compliance Reviews	Regularly update data protection practices to adapt to new regulations or changes in activities.	Schedule periodic reviews; stay informed about legal changes; involve stakeholders in review processes.	Ongoing

Table 10. *Privacy protocol summary for human participation activities*

[67] This protocol is only applicable in case of collection, storage, processing, or use of personal data. According to GDPR, Personal data is any information relating to an identified or identifiable living natural person. The various pieces of information that, when collected, can lead to the identification of a specific individual are also personal data.

- Examples of personal data are: first and last name, address, e-mail address, nombre.apellido@empresa.com, national identity card number, location data (such as the location function of a mobile phone) (*), Internet Protocol (IP) address, cookie identifier (*), telephone advertisement identifier, data held by a public authority which could be a symbol that uniquely identifies an individual.
- The following personal data are considered "sensitive" and are subject to specific processing conditions: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data processed solely for the purpose of identifying a person, data concerning health, data concerning the sex life or sexual orientation of a person.