Enhancing Copernicus Security Services –
EU governmental crisis management hub for forced population displacement

D3.1 – THEIA Ethics version 1 (1st period)

WP3 Ethics 1 - 1st period

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under GA 101190051. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Lead Contributor	Vagelis Papakonstantinou (MPL)
Contributors	Francisco Javier López Guzmán (MPL)
Reviewers	Giorgos Lampropoulos (WTOC)

Due Date	28/02/2025
Delivery Date	27/02/2025
Type	R — Document, report
Dissemination Level	PU - Public
Keywords	Ethics, benchmark legislation analysis and consent forms

Document History

Version	Date	Description	Author	Description/ Action	Validation
	24/01/2025	Outline	Francisco Javier López Guzmán (MPL)		Deliverable leader
0.1	14/02/2025	First Draft	Francisco Javier López Guzmán (MPL)	Initial draft of the contents	
0.2	25/02/2025	Draft for review	Francisco Javier López Guzmán (MPL)	Internal Review process	Consortium partner WTOC review. PC review. Feedback is collected and incorporated into the document.
0.3	26/02/2025	Final Draft	Francisco Javier López Guzmán (MPL)	Finalisation and final approval	SAB security check. Feedback is collected and incorporated into the document.
1.0	27/02/2025	Final version	Liza Panagiotopoulou (GSH)	Submission to EC	

Legal Disclaimer

Contents

Executive Summary

The current deliverable, D3.1 – THEIA Ethics version 1 (1st period), corresponds to Task 3.1 "1st period project ethics and legal aspects of THEIA" under WP3 Ethics 1 - 1st period, led by MPL Brussels. It serves as the initial iteration of the legal and ethical analysis for the THEIA project. It is part of Work Package 3 (WP3: Ethics 1 – 1st period), which focuses on developing compliance safeguards to ensure alignment with legal and regulatory requirements during the project's first period (M1–M15). The document provides a preliminary examination of ethical considerations, data protection, and privacy, ensuring adherence to key legal and ethical principles, as well as the necessary legal documentation. The primary goal of WP3 is to ensure compliance with relevant laws and regulations to minimize potential ethical and legal risks.

List of Tables

List of Figures

List of Acronyms / Abbreviations

Table 1. List of Acronyms/Abbreviations

Acronym / Abbreviation	Explanation
AI	Artificial Intelligence
AGI	Artificial General Intelligence
API	Application Program Interface
CoE	Council of Europe
ECHR	European Convention of Human Rights
ECJ	European Court of Justice
ECtHR	The European Court of Human Rights
EDPB	European Data Protection Board
EU	European Union
EUI-DPR	European Union Institutions – Data Protection Regulation
FAIR (Principles)	Findable, Accessible, Interoperable, Re-usable
GA	General Agreement
GDPR	General Data Protection Regulation
Gen-AI	Generative Artificial Intelligence
GeoAI	Geospatial Artificial Intelligence
Ibid	Ibidem: Latin for "in the same place", referring to the source cited in the preceding note or list item.
LEA	Law Enforcement Agency
LED	Law Enforcement Directive
ML	Machine Learning
OSINT	Open Source Intelligence
UAV	Unmanned Aerial Vehicles
UDHR	Universal Declaration of Human Rights
UAS	Unmanned Aerial Systems
UN	United Nations

1. Introduction

Addressing critical challenges such as population displacement due to conflicts, exacerbated by factors like climate change, extreme weather events, food shortages, and poverty, remains paramount. The implementation of THEIA, integrating data fusion, processing, and analysis, particularly leveraging Geospatial Artificial Intelligence (GeoAI) and Machine Learning, is poised to enhance the efficacy of existing services significantly. Through the amalgamation of multi-temporal data and diverse datasets, THEIA empowers better decision-making and adapts to evolving policy and user needs. This technological advancement, bolstered by GeoAI, augments detection capabilities and ensures timely access to crucial information, bridging the gap between capabilities and stringent security demands.

By integrating non-space data and end-user intelligence, THEIA's supply chains add value not only at the operational level but also at regional and local levels, facilitating improved coordination. Furthermore, THEIA catalyzes fostering EU-independent capabilities and technologies, thereby bolstering the European space ecosystem's consolidation and ensuring the sustainable coexistence of legacy and New-Space solutions. Its services cater to a wide array of end-users, including EU entities such as SatCen and Frontex, Member State Ministries of Defence, Intelligence Agencies, Police Forces, NATO, and potentially Extra-EU National and Supranational Entities such as the United Nations.

This document is the report presenting the overall first iteration of the legal and ethical analysis for project THEIA. This report is integrated in Work Package 3 (WP3 Ethics 1 - 1st period), which develops the compliance safeguards to guarantee the legal and regulatory correspondence during the first period of the research in the project (M1-M3). Ethics, data protection and privacy are covered in a preliminary approach in this report, ensuring adherence to the main ethical and legal principles and the necessary legal documentation for the research. The main objective of WP3 is ensuring compliance with law and regulations to mitigate risks.

The WP3 consists of a unique task:

- Task 3.1: "T3.1 1st period project ethics and legal aspects of THEIA" [M1-M15]. This task focuses on the description of the ethical issues connected to the development of the research in THEIA. These issues are identified and mitigated by the development of principles such as data protection and privacy awareness. These principles are developed during the first period of the project. Compliance with existing legislation is the priority and identifying the best angle for societal acceptance of the technical developments in THEIA. Legal documentation necessary to prove compliance is prepared and delivered to the consortium for internal use and external accountability.

This document is one of the outputs of **Task 3.1 "1st period project ethics and legal aspects of THEIA",** and represents the first iteration of this report. The second iteration will be the report in D.3.2 Deliverable D3.2 – THEIA Ethics version 2 (1st period), which will develop on this content.

1.1 Purpose and scope of the deliverable

The purpose of the deliverable is to develop compliance, describe the legal framework applicable to the project and expose societal and ethical aspects of interest.

The report covers the following aspects:

- The basic legislation applicable to the research in the project: covering from international treaties, covenants and fundamental rights conventions, European Union primary and secondary legislation and selected national legislation on the scope of the project.
- The main ethical concerns that the research in the project may trigger, and the societal acceptance of the technological elements developed in THEIA.
- The consent forms to collect specific consent for the participation in project demos and pilots as external representation.

1.2 Structure of the deliverable

This document consists of the following chapters:

- The executive summary of the deliverable.
- **Chapter 1** which includes a short description of THEIA objectives, purpose, scope and structure of the deliverable.
- **Chapter 2** which focuses on the most prominent legal issues and the protection under the ECHR and the EU Charter of Fundamental Rights.
- **Chapter 3** develops the right to privacy and the societal impact of the research.
- **Chapter 4** includes the right to the protection of personal data.
- **Chapter 5** focuses on the description of the main Ethical and social concerns.
- **Chapter 6** describes the relevant regulatory frameworks in Member States.
- **Chapter 7** focuses on the collection of consent for the processing of personal data
- **Annex I** includes the first version of the template for consent forms (v1).

1.3 References

- Project GA with No. 101190051
- THEIA Partners CA
- European Data Protection Board Guidelines 01/2025 on Pseudonymisation. Available at https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-012025-pseudonymisation_en
- European Data Protection Board Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Available at: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en
- European Data Protection Board Guidelines 05/2020 on consent under Regulation 2016/679. Available at https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

European Union Agency for Fundamental Rights and Council of Europe, 2018. Handbook on European data protection law, 2018 edition. Available at https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

2. Prominent legal issues and the protection under the ECHR and the EU Charter of Fundamental Rights

The research in THEIA project involves a number of research initiatives and activities with legal and societal impact. This report anticipates the areas of prominent impact, the fundamental freedoms and rights of individuals which may be affected by this research. This full impact will be revealed during the development of the research project. The present report also defines the main areas of compliance and the legislation applicable to the research at the project at three levels:

- International legal framework of protection of fundamental rights. This framework includes the European Convention of Human Rights (ECHR)[1], which is of relevance to the project due to the development of the research activity within the European Union and potentially applied within the European continent.
- European Union legal framework applicable, including the European Union Charter of Fundamental Rights (EU Charter), EU regulations and directives and other secondary legislation of applicability.
- National legislation of interest for the development of the research in the project.

Within these levels, a number of fundamental rights and freedoms may be impacted by the research activity in the project. The development of the research to enhance the Copernicus Security Services and EU governmental crisis management capabilities in the area of forced population displacement has a certain impact in the following subjects.

2.1. Rights of migrants

Displaced population, economic migrants and refugees have a number of rights recognised under European Union legislation. Public authorities need to abide by those while developing borders management, security policies and other public policy related to the displaced population.

On the European continent, the international framework is of important relevance as set by the European Convention of Human Rights (ECHR). Although the EU itself as an international organisation is not a member of the Council of Europe, all of the 27 EU Member States are members also of the Council of Europe. This situation implies that the Convention, which is a treaty binding all the members of the Council of Europe, also binds the EU members. But the actions of the European Union institutions cannot be yet subject to scrutiny by the European

[1] Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols No. 11 and No. 14, Rome, 4 November 1950, ETS No. 5. http://conventions.coe.int/treaty/en/treaties/html/005.htm

Court of Human Rights (ECtHR), which is part of the institutional framework of the Council of Europe.[2] This situation is on development and under political negotiation[3], considering the legal mandate under Protocol (No 8) of the Treaty on European Union, incorporated by the Lisbon Treaty of 2009.

Considering this background, the ECHR framework is of importance and reference when the rights and freedoms of the European citizens and migrants in European territory are concerned.

The regulation of fundamental rights and freedoms in Europe is deeply influenced also by the European Union Charter of Fundamental Rights (EU Charter). The EU Charter is a legally binding text to all 27 Member States of the European Union, as part of the acquis communautaire of the EU. Specifically, when developing and implementing EU legislation. Its application does not conflict the development of the Council of Europe legal framework.

While developing policy and public activity that affects displaced population, it is important to consider the fundamental rights and freedoms regulated under the ECHR and the EU Charter:

- Right to Life (Article 2 ECHR) – Everyone's right to life shall be protected by law. This right may cover the rights of migrants in the territory of application of the ECHR, which may prevent their unlawful deportation to places where a person may face a tangible risk of death.
- Prohibition of Torture and Inhuman or Degrading Treatment (Article 3 ECHR) – The ECHR prohibits these conducts, which may also cover the risk of migrants being subject to them if they are deported or expulsed to a third country if they suffer these consequences. Regarding these practices, the case law established by the European Court of Human Rights in its decision Soering v. United Kingdom (1989)[4] is of importance, on the prohibition of extradition to a country where the applicant faced inhuman or degrading treatment, as well as the Chahal v. United Kingdom (1996)[5] case on the category of absolute prohibition. As well as on the human conditions of treatment in migrant detention centers in M.S.S. v. Belgium and Greece (2011).[6]
- Right to Liberty and Security (Article 5 ECHR) – Forcefully displaced population may suffer a risk to their liberty and security if they are placed under arrest in an unlawful way. This right protects them against arbitrary detention, including in immigration detention

[2] See official information from the Delegation of the European Union to the Council of Europe. Available at: https://www.coe.int/en/web/portal/eu-accession-echr-questions-and-answers
[3] See official information from the Council of Europe on the matter. Available at: https://www.coe.int/en/web/portal/eu-accession-echr-questions-and-answers
[4] Soering v United Kingdom (1989) 11 EHRR 439.
[5] Chahal v United Kingdom (1996) 23 EHRR 413.
[6] MSS v Belgium and Greece (2011) 53 EHRR 28.

centers. Only when and under the circumstances foreseen in the law, or mandated by a court of justice, these detentions may take place. The ECHR only foresees unauthorised entry into the country, procedures of deportation or extradition as justified for these detentions.

- Right to Respect for Private and Family Life (Article 8) – This right needs to be specifically considered in cases where deportation would break up families or disrupt lawful entry and long-term residence in a European country. The implications for the processing of personal data and right to privacy will be studied furtherly in this report.
- Prohibition of expulsion of nationals and prohibition of collective expulsion (Articles 3 and 4, Protocol No. 4 ECHR) – This right prevents states from expelling groups of migrants without individual assessments. The ECtHR has developed this prohibition with regards of the collective expulsions of migrants intercepted at sea at case Hirsi Jamaa and Others v. Italy (2012).[7] The content of this right is in relation to the EU development in article 19 of the EU Charter, on the protection in the event of removal, expulsion, and extradition, which also prohibits collective expulsions and prevents deportation to countries where individuals risk torture, inhuman treatment, or the death penalty.
- The right to asylum. Article 18 of the EU Charter develops the right to international protection of migrants, in relation with the rules of the Geneva Convention of 28 July 1951 (Convention Relating to the Status of Refugees), and the Protocol of 31 January 1967 relating to the status of refugees. This right is of special criticality for the forcefully displaced population and is in relation to the United Nations multilateral legal framework. This right is explored and delimited by the EU Court of Justice in cases C-528/15 *Al Chodor*[8] on the clarification on the legal criteria for detaining asylum seekers in the EU, C-638/16 PPU X. and X. v. Belgium[9] on the non-obligation of EU Member States to issue humanitarian visas to people seeking asylum, and C-333/13 *Dano*[10], which allowed EU Member States to deny social benefits to economically inactive migrants who move to an EU country without sufficient resources.

The European Court of Human Rights (ECtHR) has developed case law that strengthens these protections for migrants, refugees, and asylum seekers if they integrate the forcefully displaced population. Specifically, on the required individualised guarantees before transferring asylum seekers outside of the EU to avoid degrading treatment[11] and on the limits on pushbacks at

[7] Hirsi Jamaa and Others v Italy (2012) 55 EHRR 21.
[8] Case C-528/15 Al Chodor and Others [2017] ECLI:EU:C:2017:213
[9] Case C-638/16 PPU X and X v État belge [2017] ECLI:EU:C:2017:173
[10] Case C-333/13 Dano v Jobcenter Leipzig [2014] ECLI:EU:C:2014:2358.
[11] Tarakhel v Switzerland (2014) 60 EHRR 28.

borders, ruling that summary expulsions could be justified if migrants bypassed legal entry procedures.[12]

The European Union legal framework has an extensive protection to forcefully displaced population in the rights and freedoms abovementioned. Additionally, general rights in the EU Charter, such as human dignity (Article 1), non-discrimination (Article 21), and fair working conditions (Article 31), also apply to migrants who are potentially in this situation. These rights are delimited by the EU Court of Justice in important cases such as Case C-34/09, *Zambrano*[13] on the respect for family life in the case of mixed families with an EU and non-EU background. Case C-256/11, *Dereci*[14] (2011) clarified the doctrine in these cases, limiting protection to cases where expulsion would force an EU citizen to leave the EU.

2.2. Freedom of assembly and association

Considering the development of technologies that analyse large crowds in project THEIA, some assembling of people at a large scale could be seen as a potential threat for European borders. The use of the technologies developed in project THEIA with that priority may hinder the correct development of the freedom of assembly and association of citizens, specifically forcibly displaced population. Article 11 of the European Convention of Human Rights protects this right, specifically with regards to peaceful assembly and the freedom of association with others. This right is also enshrined in the European Union Charter of Fundamental Rights (EU Charter), pursuant to Article 12. The specificity of this article in the EU Charter is related to the protection in particular with regard to political, trade union and civic matters.

2.3. Freedom of thought, conscience and religion

Forcibly displaced population may integrate a heterogeneous population, or a homogeneous group of people with a particular origin and cultural background. The use of Open source Intelligence (OSINT) may target specific populations, affecting their freedom of thought, conscience and religion, influencing a self-conscious attitude or directly discriminating people based on the content shared online about their political beliefs, trade union association or religion. In this regard, the use of these technologies should consider the content of the protections developed in article Article 9 ECHR. The limitations to this right can only be developed when directly prescribed by law, and when the limitation is necessary in a democratic society, in

[12] ND and NT v Spain (2020) 72 EHRR 29.
[13] Case C-34/09 Gerardo Ruiz Zambrano v Office national de l'emploi (ONEm) [2011] ECR I-1177
[14] Case C-256/11 Dereci and Others v Bundesministerium für Inneres [2011] ECR I-11315.

light of paramount interests such as public order or protection of rights and freedom of others. Article 10 of the EU Charter protects the freedom of thought, conscience and religion, and the right to conscientious objection related to it.

3. The fundamental right to privacy in connection with the research in THEIA

The previous list of the fundamental rights' legal framework in the scope of the THEIA project is not exhaustive. The research in project THEIA involves the development of technological solutions that may affect various spheres of life, and different aspects of rights and freedoms of individuals. One merits special attention: the fundamental right to privacy. Considering the extensive use of data (and particularly personal data) that the technologies that may be developed in project THEIA imply, the right to privacy may be specifically affected. The use of satellite video and multispectral images, the exploration of crowdsourcing and open-source data from social networks and the use of Geospatial Artificial Intelligence (GeoAI), amongst others, merits this specific look into the legal framework on the right to privacy that may apply to project THEIA.

3.1. Historical and background information

The right to privacy was first signalled amongst the legal literature by American authors Samuel D. Warren & Louis D. Brandeis, in their paper "*The Right to Privacy*"[15], as early as the year 1890. This academic paper is considered amongst scholars as the first recognition of the right to a private life, the boundaries of the activity of the State with regards to the private life of its citizens, and the family rights connected to this reality. After some analysis of the issue, the authors fundamentally defined the right to privacy as "*the right to be left alone".*[16]

The modern academic literature distinguishes specific characters further to this aphorism. Professor Daniel Solove characterises in his work: "*Understanding Privacy*"[17] the following elements:[18]

- The right be let alone, that is "to live one's life as one chooses, free from assault, intrusion or invasion except as they can be justified by the clear needs of community living under a government of law"[19];

[15] Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, in Harvard Law Review, 1890, Vol. 4, No. 5, p 193-220.
[16] Ibid. p. 195.
[17] Daniel J. Solove, Understanding Privacy – Chapter 2: Theories of privacy and their shortcomings, Cambridge Massachusetts: Harvard University Press, 2008. P. 2.
[18] This summary is extracted from report S. Roda, I. Böröcz, HR-Recycler. D 2.1. Report on security, data protection, privacy, ethics and societal acceptance, p.10, and a cross-reference of report F.J. López-Guzmán, INTREPID D.3.1, Data Protection, Privacy, Ethics and Societal Acceptance v1, p. 8.
[19] Justice Abe Fortas as cited in Ibid. p. 2.

- The limited access to the self, as the ability to shield oneself from unwanted public observation and discussion by others;
- Secrecy, where privacy is infringed by public disclosure of previously concealed information and where the interest of the individual is to avoid disclosure of personal matters;
- Control over personal information, meaning the claim of individuals, groups or institutions to determine how, when and to what extent information about them is given to others;
- Personhood, concerns the protection of the integrity of personality and considered to be "those attributes of an individual which are irreducible in the selfhood"[20]; and,
- Intimacy, where the focus is on the development of personal relationships and different degrees of intimacy and self-revelation.

In the legal context, the Universal Declaration of Human Rights (UDHR), adopted in 1948, enshrined the right to privacy as one of the fundamentally protected human rights. Soon after adoption of the UDHR, Europe too affirmed this right – in the European Convention on Human Rights (1950). Under the case law, according to the ECtHR and the CJEU, the term 'private life' must not be interpreted restrictively.[21] "However, the assessment of whether or not there is, or has been, an interference with "private life" depends on the context and facts of each case."[22]

3.2. Universal Declaration of Human Rights

Article 12 of the UDHR:

> *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*

The Universal Declaration of Human Rights (UDHR) is the primary international reference for the protection of fundamental rights in the world. This legal instrument integrates the main set of general principles established internationally for the protection of fundamental rights. Its content is applicable *erga omnes*, this means regardless of the participation of the states in the United Nations institutional framework. It protects all human beings and is the standard of the application of and protection of rights all around the world. The inclusion of the right to privacy

[20] Ibid. p.9.
[21] J. Kokott and C. Sobotta. The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. International Data Privacy Law, 2013, Vol. 3, No. 4. P. 223.
[22] Ibid, p. 20.

in its legal setup marked the first iteration of this right in the international legal framework, and elevates the matter to a primary protection that needs to be considered in every region in the world.

3.3. European Convention of Human Rights

Article 8 of the ECHR:

> *Right to respect for private and family life*
>
> *1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *2.There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

The Council of Europe was created after the Second World War to bring together the states of Europe to promote the rule of law, democracy, human rights and social development. This International Organisation was the shoot, together with the European Coal and Steel Community, of what it later became the European Union. The CoE impulsed, with this purpose, the creation and adoption of the European Convention on Human Rights in 1950, which entered into force in 1953. As of 2025, the Council of Europe comprises 46 Contracting Parties (after the recent dismissal of the Russian Federation in 2022), 27 of which are also EU Member States (excluding the United Kingdom, who abandoned the European Union as per 31st January 2020). Contracting Parties must respect the rights contained in the ECHR when exercising any activity or power.

The creation of the ECHR led to the establishment of the European Court of Human Rights (ECtHR). It was set up in 1959 and is based in Strasbourg, France. The ECtHR ensures that states observe their obligations under the Convention by considering complaints from individuals, groups of individuals, NGOs or legal persons alleging violations of the convention.[23]

The second paragraph of Article 8 of the ECHR established that the right to privacy can be limited due to three requirements:

1. need for a legal basis (legality requirement)

[23] European Union Agency for Fundamental Rights and Council of Europe, 2018. Handbook on European data protection law, 2018 edition. < https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf > [“Handbook on European data protection law”] accessed 25 February, 2025. P. 18.

2. interference with a legitimate aim (legitimacy requirement) and
3. necessary in a democratic society.

Moreover, the respect for private life is not an absolute right. The exercise of the right to privacy could compromise other rights, such as freedom of expression and access to information. It is the Court's mission to find a balance between the different rights at stake.

3.4. Charter of Fundamental Rights of the European Union

Article 7 of the Charter:

> *Respect for private and family life*
>
> *Everyone has the right to respect for his or her private and family life, home and communications.*

Article 52 of the Charter:

> *Scope and interpretation*
>
> *1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.*
>
> *(…)*

3. In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.

The EU Charter of Fundamental Rights enumerates all the personal, civic, political, economic and social rights enjoyed by people within the EU. It entered into force in December 2009 with the signature of the Treaty of Lisbon and covers all the rights found in the case law of the Court of Justice of the EU the rights and freedoms contained in the European Convention on Human Rights other rights and principles resulting from the common constitutional traditions of EU countries and other international instruments.

Article 7 of the Charter is almost identical to the article 8 of the ECHR. It is complemented by article 52 of the Charter that specifies limitations of the right to privacy. These limitations are also similar to those provided in the ECHR and allowed if:

1. it is provided by law;
2. respect the essence of the right to privacy;
3. proportional and necessary;
4. meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

The provisions of the Charter are addressed to the institutions and bodies of the European Union with due regard for the principle of subsidiarity. It is also addressed to the Member States only when they are implementing the Union law. Therefore, the Charter provides a basis for the EU legislation, including GDPR, as explained further.

4. The right to the protection of personal data

4.1. Background information

The protection of personal data is a fundamental right, ensuring that individuals are safeguarded against unlawful processing of their information. At the European level, legal protections for data privacy derive from the provisions already exposed in the previous sections on the European Convention on Human Rights (ECHR). Within the European Union, from the EU Charter of Fundamental Rights respectively, which explicitly establish the right of individuals to the protection of their personal data.

While data protection and privacy are closely related, they are recognized as distinct rights in legal frameworks worldwide. Data protection emerged from the right to privacy, and both serve as essential mechanisms to uphold fundamental values such as freedom of expression and freedom of assembly.

The key distinction between these rights lies in their legal scope and implementation. The right to privacy is broadly framed as a prohibition on interference, with exceptions permitted under certain public interest justifications. In contrast, data protection is a proactive and structured right, requiring a system of checks and balances to safeguard individuals when their personal data is processed. This system ensures compliance through independent oversight and the enforcement of data subject rights.

Within the EU, primary legislation such as the Charter of Fundamental Rights and the TFEU lays the constitutional foundation for data protection. The General Data Protection Regulation (GDPR)[24] serves as the main secondary legislation regulating data processing. Several key institutions contribute to the interpretation and enforcement of these rules, including at an European level:

- European Data Protection Supervisor (EDPS): The independent data protection authority of the EU, responsible for monitoring and ensuring compliance with privacy regulations, advising EU bodies on data protection matters, and assessing the impact of emerging technologies on personal data protection.
- European Data Protection Board (EDPB): A supervisory body established under the GDPR, ensuring the harmonized application of data protection rules across Member States. The EDPB replaced the Article 29 Working Party and facilitates cooperation between national data protection authorities.

[24] 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, OJ L 119, 4.5.2016, p. 1–88.

4.2. Principles, rights and obligations under the GDPR

4.2.1. Core definitions

To ensure legal clarity in the THEIA project, it is crucial to reference the definition key data protection concepts, as they determine the applicable legal framework. The GDPR (Articles 4, 9, 22 and Recital 51) provides the following definitions:

Table 2. Core definitions in GDPR

Concept	Definition
"Personal data"	Any information relating to an identified or identifiable natural person (data subject).
"Identifiable natural person"	Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier (e.g. IP addresses) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
"Data subject"	Any natural person whose personal data is being processed.
"Biometric data"	**Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data (finger print identification).**
"Data concerning health"	**Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.**
"Sensitive data"	**Personal data which are, by their nature, particularly sensitive as the context of their processing could create significant risks to the fundamental rights and freedoms. It may include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.**
"Data controller"	**A natural or legal person who, alone or jointly, determines the purposes and means of processing.**

"Data processor"	**A natural or legal person who processes personal data on behalf of the controller.**
"Processing"	**Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.**
"Profiling"	**Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.**
"Automated individual decision-making"	**Decision based solely on automated processing, including profiling, which produces legal effects concerning data subject or similarly significantly affects him or her.**
"Pseudonymisation"	**Processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.**
"Consent of the data subject"	**Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.**
"Personal data breach"	**Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed**

Given the broad scope of the definitions of personal data and processing, the THEIA project must assess whether the data it collects—including geospatial data—falls under the scope of application of GDPR. If so, all GDPR obligations are of application. Additionally, sensitive data (e.g., biometric and health data) is subject to stricter legal requirements.

Anonymous data falls outside the GDPR's scope, as it does not relate to an identifiable individual. While anonymization can be legally advantageous, making compliance easier, true anonymization is often challenging and may reduce data usability for research. The feasibility of anonymization will be assessed during system design to balance legal compliance with research utility.

4.2.2. General principles

The GDPR pursues two primary objectives:

- Protecting individuals' personal data
- Ensuring the free movement of data within the EU

To achieve these goals, the GDPR sets out seven fundamental principles for data processing in article 5 GDPR:

Table 3. General principles in GDPR

Principle	Explanation
Lawfulness, fairness and transparency[25]	Data must be processed lawfully, fairly, and transparently. Controllers must notify individuals about processing activities and ensure compliance with GDPR standards.
Purpose limitation[26]	Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in an incompatible manner.
Data minimisation[27]	Only the minimum amount of personal data necessary for a specific purpose should be collected and processed.
Accuracy[28]	Data must be accurate and up-to-date. Incorrect or outdated data must be corrected or deleted.
Storage limitation[29]	Personal data must be retained only for as long as necessary for its intended purpose.

[25] GDPR, Art. 5(1)(a)
[26] Ibid, Art. 5(1)(b).
[27] GDPR, Art. 5 (1)(c).
[28] GDPR, Art. 5 (1)(d).
[29] GDPR, Art. 5(1)(e).

Integrity and confidentiality[30]	Data must be securely processed to prevent unauthorized access, disclosure, or destruction.[31]
Accountability[32]	Data controllers must demonstrate compliance with all GDPR principles, including keeping records of processing activities, appointing a Data Protection Officer (DPO), and implementing security measures.[33]

4.2.3. Legal Grounds for Processing

To comply with the principle of lawfulness, personal data processing must be based on at least one of the legal grounds outlined in Article 6 of the GDPR:

1. Consent of the data subject
2. Performance of a contract to which the data subject is party
3. Compliance with a legal obligation to which the controller is subject
4. Necessity to protect vital interests (e.g., saving lives in emergency situations)
5. Necessity for the performance of a public interest task
6. Processing is necessary for the purposes of the legitimate interests pursued by the controller

When processing sensitive data, stricter conditions apply (Article 9 GDPR).

4.2.4. Rights of Data Subjects

Under GDPR, individuals have rights regarding their personal data, defined in Chapter III GDPR, including:

- Right to be informed (controllers must provide clear information about data processing)
- Right of access (data subjects can request access to their data)
- Right to rectification (inaccurate data must be corrected)
- Right to erasure ('right to be forgotten')
- Right to restrict processing
- Right to data portability

[30] GDPR, Art. 5(1)(f).
[31] Ibid.
[32] GDPR, Art. 5(2).

- Right to object
- Right to lodge a complaint

4.2.5. Obligations of Data Controllers

Data controllers must ensure compliance with GDPR by implementing, amongst others:

- Data protection by design and by default
- Records of processing activities
- Security measures
- Incident reporting (data breach notifications)

4.3. Law Enforcement Directive

The development of the scientific research in project THEIA aims at providing assistance to end-users enhancing Copernicus Security Services that may be applied to the management of EU governmental crises under forced population displacement. This research area enters straight into the scope of application of the Law Enforcement Directive[34], as defined in its article 1(1). This article determines the application of the Directive when both its personal and material scope are met. Specifically, the material scope covers data processing for the following purposes:

1. Prevention, investigation, detection, and prosecution of criminal offences.
2. Execution of criminal penalties.
3. Safeguarding against and prevention of threats to public security.

If none of these criteria are not satisfied, the Directive does not apply, and instead, the General Data Protection Regulation (GDPR) or other EU instruments may regulate the processing of personal data. Forced population displacement management enters directly into the competences of the Law & Order forces and law enforcement public agents. Considering the development of the technical capabilities in project THEIA, it is very likely that these technologies are utilised by end-users in activities that fall into the scope of the Directive. Therefore, the conditions for the processing of personal data will be triggered, and the safeguards of the Directive would need to be applied.

[34] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.

The Directive the competent authorities as any public authority competent for the abovementioned activities, or any other body entrusted by EU law or Member States' law to exercise public powers in the context of those activities.[35] The Law Enforcement Directive largely reflects the data protection principles established in the GDPR, while providing exceptions and restrictions to data subjects' rights in accordance with its scope and the underlying law enforcement goals:

1. Prohibition of Automated Decision-Making with Legal Effects (article 11 LED): The Directive prohibits decisions based solely on automated processing, including profiling, if they produce adverse legal effects on individuals. This is a parallel right to article 22 GDPR, that ensures human oversight of technologies such as GeoAI. However, such processing may be allowed if explicitly authorized by law and subject to appropriate safeguards, including human intervention.
2. Principles of Data Processing (article 4 LED): comparable to those contained in GDPR sections 1 to 4, such as purpose limitation, the processing of personal data only for ensuring data is processed only for specific, legitimate purposes, data minimization applies, that bound public entities that develop law enforcement.
3. Special Protections for Sensitive Data (article 10 LED): The processing of special categories of personal data (e.g., racial or ethnic origin, political opinions, religious beliefs) is prohibited unless strictly necessary and subject to additional safeguards. Discriminatory profiling based on sensitive data is explicitly banned.
4. Logging and Accountability (article 25 LED): Law enforcement databases must maintain logs of processing activities to ensure oversight and accountability. Logs serve as a safeguard against unauthorized access and can be used as evidence in investigations of data breaches.
5. Independent Supervision (article 45 LED): each Member State must designate an independent supervisory authority to monitor compliance with the Directive. These authorities have enforcement powers, including the ability to investigate complaints and impose corrective measures.
6. Rights of Data Subjects (articles 13-17 LED): comparable to those contained in GDPR Chapter III, with certain specificities. Data subjects have rights to access, rectification, and erasure of their personal data, amongst others. If access is restricted for law enforcement reasons, individuals may exercise their rights through the supervisory authority.

[35] Juraj Sajfert and Teresa Quintel, 'Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities' (2019) forthcoming in Cole/Boehm GDPR Commentary, Edward Elgar Publishing https://ssrn.com/abstract=3285873 accessed 24 February 2025.

7. International Data Transfers (articles 35-39 LED): specific rules applicable to the transfer of personal data to foreign entities in the scope of law enforcement, only when an adequate level of protection is ensured. There are special rules that apply for asymmetrical transfers, allowing law enforcement agencies to request data directly from private entities in third countries.

4.4. EUI-DPR

Some entities involved in the research in project THEIA have a public nature. Specifically, they integrate the European Union's institutional framework. This means that they have their own rules for internal functioning and organisation, often created ad hoc for the institutions through specific legislative procedures. One of the aspects of different development to the research involvement of private entities in THEIA is the processing of personal data.

Processing of personal data by EU institutions is outside of the scope of application of GDPR. There is a specific regulation that governs this processing: the European Union Institutions – Data Protection Regulation (EUI-DPR)[36]. This legal framework was adopted in 2018, when GDPR was already in force. It mirrors the basic content of GDPR, with only few specificities applicable to public bodies of the European Union. These bodies do not include Member States national institutions, regardless of the possibility of their application of EU law:

1. Supervisory Authorities: GDPR is enforced by national Data Protection Authorities (DPAs) within each Member State, which oversee compliance and address breaches within their respective jurisdictions. On the other hand, the EUI-DPR's oversight is provided by the European Data Protection Supervisor (EDPS), an independent EU body responsible for monitoring the application of data protection rules by EU institutions and bodies.
2. Legal Basis and Framework: GDPR establishes a comprehensive legal framework for data protection across the EU, harmonizing laws to facilitate the free flow of personal data while protecting individual rights. EUI-DPR, however, aligns closely with the GDPR to ensure consistency but is tailored to the specific operational needs and structures of EU institutions and bodies.
3. Operational Data Processing: GDPR addresses general personal data processing activities across various sectors, while EUI-DPR includes specific provisions (notably Chapter IX) that pertain to the processing of operational personal data by EU bodies when carrying out

[36] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, PE/31/2018/REV/1, OJ L 295, 21.11.2018, p. 39–98.

activities related to the prevention, investigation, detection, or prosecution of criminal offenses.

4. The legal bases for the processing of personal data under EUI-DPR are the following: a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body; necessity for compliance with a legal obligation to which the controller is subject; performance of a contract, consent to the processing, protection of the vital interests of the data subject or of another natural person (article 4 EUI-DPR). There is a clear pre-eminence of the legal mandates and performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body. Legitimate interest, which is an existing legal basis under article 5(1)(f) GDPR.

The EUI-DPR will only be applied in project THEIA to the extent that is necessary to delimitate and comply with the involvement of these EU public bodies in the research of the project. For all the rest of the activities, the processing of personal data will be structured and complied through GDPR, the LED Directive and the AI Act, when applicable respectively.

4.5. Processing of personal data within the different technological solutions of THEIA

4.5.1. Processing of personal data within the processing of satellite data and UAV/UAS

Satellites can be used for earth observation using space technologies. Satellites orbiting the Earth can generate various types of images:[37]

- Optical (Visible Light) Images: These images are similar to conventional photographs. They capture reflected sunlight in the human visible spectrum. They can be used for mapping, urban planning, and environmental monitoring. They may be of limited use depending on weather conditions, since their view can be obstructed by clouds and are based on daylight availability.
- Infrared (Thermal) Images: These images detect heat radiation emitted by objects, rather than reflected sunlight. The images may be able to identify human beings from animals and other living creatures depending on the exactitude and power of the sensors. They may be useful for climate monitoring, vegetation analysis, and military surveillance. Some

[37] Classification created using information contained in: Elisa Celia González Ferreiro and Rafael Moro Aguilar, 'Cuestiones jurídicas entorno a la delimitación del espacio ultraterrestre' (2024) 4 Revista Española de Derecho Aeronáutico y Espacial 275-290 and Roser Almenar Rodríguez, 'Cuestiones jurídicas de seguridad nacional en el marco de las actividades de teleobservación en la era del New Space' (2024) 4 Revista Española de Derecho Aeronáutico y Espacial 301-329.

events that may be detected by a satellite using these images are wildfires, urban heat islands, and pipeline leaks.

- Multispectral and Hyperspectral Images: Satellites can capture multiple bands across the electromagnetic spectrum.
    - Multispectral: Typically 3-10 bands (e.g., Landsat, Sentinel-2).
    - Hyperspectral: Hundreds of narrow bands, providing more detailed material composition analysis.

  Their applications range from agriculture, geology, mineral exploration, and environmental assessment.
- Radar (SAR – Synthetic Aperture Radar) Images: Satellites can use microwaves to generate images, allowing operation day and night and through clouds, smoke, and vegetation. These technologies are typically used for disaster monitoring (floods, landslides, earthquakes) and military reconnaissance, as well as ice monitoring in the polar regions.
- LiDAR (Light Detection and Ranging) Images: This technology uses laser pulses broadcasted by the satellites sensors to map surfaces in 3D. They can be used to generate high-resolution topographic data. Their applications are forestry, archaeology and infrastructure monitoring.
- Ultraviolet and X-ray Imaging: They are not commonly used in Earth observation. But they can be used in astronomy and atmospheric studies. They can detect cosmic radiation, auroras, and ozone layer changes.
- Microwave and Radio Imaging: Their use may be developed for climate monitoring, sea surface temperature, and atmospheric studies. Since they can penetrate clouds and precipitation, they are useful in hurricane tracking and oceanography.

All these types of images may be used to improve the capabilities of governmental crisis management in the area of forced population displacement. The administration of borders and the control of displaced population may be benefited by the insight of fixed images and real time images that are generated by these satellites. Only those of significant impact for humans may be of interest for the scope of the current report. From the previous list, only the following could identify human beings from other living creatures or objects:

- Optical (Visible Light) Images: The use of these images may differentiate humans, and potentially be used to verify or identify individuals. Their use should be subject to all applicable existing privacy regulations similarly to imaging captured by regular cameras installed in urban areas, and should benefit from the specific safeguards needed in the use of facial recognition. Since they may be of limited use depending on weather

conditions, and their capture may be hindered by clouds and are based on daylight availability, they probably could not be the primary use of satellite data. In the event of the use of very good resolution and acceptable images where individuals could potentially be identified, the complete legal framework for the protection of privacy of individuals with regards to the processing of personal data could be triggered. Particularly if these data are not anonymised. In this regard, it is important to note the reference of the European Data Protection Board Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement.[38]

- Infrared (Thermal) Images: Human presence could be detected studying the heat radiation emitted by their bodies. These data could be used for identification if the data can be matched with that of the same person in a different circumstance. However, considering the current development of the technique and the state of the art, it is highly unlikely that a person may be uniquely identified using only the heat signature obtained by a satellite sensor.

As for the rest of types of emission (Multispectral and Hyperspectral Images, Radar (SAR – Synthetic Aperture Radar) Images and microwaves emissions, LiDAR (Light Detection and Ranging) Images, ultraviolet and X-ray Imaging and Microwave and Radio Imaging) they are of difficult use to differentiate human beings from other living creatures or objects. The identification of individuals using those emissions from artificial satellites would require capabilities that are not available in the current state of the art.

It is important to consider that the use of these technologies through artificial satellites, Unmanned Aerial Vehicles (UAV) and Unmanned Aerial Systems (UAS) is regulated in a number of international treaties.[39] These legal instruments are of broad content for the development of artificial satellites. Its content may be applicable, to some extent to the research activity in project THEIA related to these issues:

- The Outer Space Treaty (1967). Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies. This treaty establishes the outer space as a global commons space, free for exploration and use by all nations. It prohibits national sovereignty claims over celestial bodies, and it holds states responsible for national space activities, including those by private entities under its jurisdiction.

[38] European Data Protection Board Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Available at: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en .

[39] Xavier Llanas Nicolás, 'International space law and the new space age: Contemporary challenges for the current legal regime' (2024) Revista Española de Derecho Aeronáutico y Espacial, 339-380.

- The Rescue Agreement (1968). Agreement on the Rescue of Astronauts, the Return of Astronauts, and the Return of Objects Launched into Outer Space. This international agreement requires states to assist astronauts in distress and safely return them. It provides for the return of space objects that have landed in foreign territories.
- The Liability Convention (1972). Convention on International Liability for Damage Caused by Space Objects. It establishes absolute liability for damage caused by a space object on Earth's surface. It imposes fault-based liability for damage caused in space.
- The Registration Convention (1976). Convention on Registration of Objects Launched into Outer Space. This legal text requires states to register satellites and other space objects with the UN, in order to improve traceability and accountability in space activities.
- Several UN General Assembly resolutions further define state responsibilities in satellite operations. However, these resolutions lack international binding effect and are mere statements from the UN General Assembly with limited coercion power or possibility of imposition over states.
    - The Remote Sensing Principles (1986) regulate Earth observation satellites.
    - The Broadcasting Principles (1982) apply to satellite communications.
    - The Nuclear Power Sources Principles (1992) govern nuclear-powered satellites.

4.5.2. Processing of personal data with the use of satellite video and multispectral images

Images obtained through artificial satellites used to be stall images, with no development in time or video sequence capabilities. The current state of the art allows for powerful cameras to be installed in UAS that can emit and receive video feed. This video feed uses mostly Satellites Optical (Visible Light) Images. This video feed is similar to conventional video recording using regular photo-sensitive cameras. They capture reflected sunlight in the human visible spectrum in real-time motion. These images may be used for mapping, urban planning, and environmental monitoring, similarly to stall optical images. They suffer from the same limitations of optical stall images. They may be of limited use depending on weather conditions, since the view of the cameras can be obstructed by clouds and are based on daylight availability.

The current state of the art allows for powerful imaging to be displayed through cameras installed in artificial satellites. However, the resolution currently obtained cannot match close video feed in terrestrial cameras. Even with the use of Very high-resolution (VHR) optical imaging, it is not at the reach of the current state of the art to uniquely identify an individual through satellite

video images without the use of other image feed to support the identification procedure.[40] In the event that this video feed could potentially be used to identify individuals, the complete legal framework for the protection of privacy of individuals with regards to the processing of personal data could be triggered. These images would be treated as personal data in application of the EU General Data Protection Regulation and the Law Enforcement Directive.

4.5.3. Processing of personal data with the use of automated detection and identification of objects through satellite video and multispectral images

Automated detection of objects and people using image and video feed from artificial satellite sensors are areas to be explored in the current research of the project THEIA. This detection could be of potential impact for the rights and freedoms previously explained considering the possibilities of hindering the right to privacy of individuals. Only those technologies that would allow the marking of human beings in the video feed could impact these realities, mostly Satellites Optical (Visible Light) Images. And in the development of Very high-resolution (VHR) optical imaging that would allow the maximum resolution and information gathered from the video feed.

The automated detection should be developed using algorithms trained to separate different objects from human shapes and other living creatures. The training of these algorithms would need vast amounts of data and could pose risks if the data is not selected properly, with implications in Intellectual Property rights and the access to personal data. However, considering the current state of the art and capabilities of the technical equipment, the most likely scenarios are the impossibility of uniquely identifying a person in real time through these technologies. In the event that the identification would be possible individually, the complete set of privacy and data protection rules contained in the EU General Data Protection Regulation and the Law Enforcement Directive would be applicable, with special attention to the EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement.

4.5.4. Processing of personal data with the use of crowdsourcing and open-source data from social networks

Project THEIA is exploring the strengthening of Copernicus Security Services and EU governmental crisis management capabilities in the area of forced population displacement through a variety of technology solutions. These technology solutions include the use of crowdsourcing and open-source data from social networks. Crowdsourcing may be defined as

[40] M. Bennett, et al., (2022). Improving satellite monitoring of armed conflicts. Earth's Future, 10, e2022EF002904. P. Füreder, et al., (2015). Monitoring Displaced People in Crisis Situations Using Multi-temporal VHR Satellite Data During Humanitarian, Operations in South Sudan. GI Forum, 391-401.

the externalisation of the generation of information to third parties. It is a constant in the social media industry, where the users are at the same time content creators that generate information within the platform. It plays a specific role in the training of AI models. Social networks contain a vast amount of information about individuals. Depending on the nature of these data, the information may be available for the public or it may be of limited access or use under Intellectual Property limitations or personal data limitations.

Information about people´s displacement and movement is openly shared in social media, as it is for almost every aspect of human life. Be it through posts mentioning human activity and interaction around borders, or pictures and videos of groups of peoples who are displaced, there is information of interest available publicly in social media about forced population displacement. The main technical challenge is processing and filtering relevant information while ensuring compliance with privacy safeguards, social media platform terms, and intellectual property rights. For example, this may involve anonymizing social media posts to protect user identities.

In that sense, it is important to note that not all publicly available information is free to be used and processed. The fact that information is shared on social media publicly does not mean that the author is licensing its use or giving away his/her privacy rights. Additionally, social media platforms typically block the access to this information at an industrial scale in their Terms of Service. Some platforms provide official APIs that allow researchers and developers to access data under certain conditions.

Data scraping and repurposing this data requires a very solid legal basis, often considering public order and public interest exceptions, or specific user consent. Truly open-source data under licenses like Creative Commons (CC BY-SA), allows the direct reuse of the information under specific conditions. But few publicly accessible websites or social media platforms allow for this use (Wikipedia, OpenStreetMap amongst others). Data scraping could be considered the unlawful development of crowdsourcing, which is the subject of current lawsuits all around the world which confront the views of users and data brokers, as well as the platforms that host this content.[41]

Crowdsourcing may imply the processing of personal data. When accessing publicly available information on the internet, information is very often mixed with personal data, in the sense defined by the EU General Data Protection Regulation in its article 4(1). The processing of these personal data can only be developed with very specific legal grounds, defined as legal basis under article 6 GDPR. Crowdsourcing including personal data is a practice of difficult accommodation to these legal bases. Legitimate interest has been explored by some entities that have developed crowdsourcing using social media data. However, it has been pushed back by regulators in the

[41] One example is the recently ruled case in the courts of the United States of America Court of Appeals for the Ninth Circuit., HiQ Labs, Inc v LinkedIn Corp, 31 F.4th 1180 (9th Cir 2022).

European Union as an unadvisable practise.[42] Some authors[43] have discussed the possibility of the use of the freedom of information exception for the development of crowdsourcing, or even data scraping, using personal data. This could constitute an exception and fall under the umbrella of article 6(1)(e) GDPR for a task carried out in the public interest.

However, accommodating such practises in relation to massive amounts of information that are needed to boost border control capabilities could be a legal challenge. Even so, with a greater risk for fundamental rights of individuals if this oversight extends to the processing of special categories of personal data as defined in article 9 GDPR. The most realistic scenario would be that these practices should be limited to open-source data and strictly non-personal data in order for them to be lawful in the European Union.

If these practices need to involve the processing of personal data, they could only be developed with a high degree of legal certainty if they would fall outside of the scope of application of GDPR, when the activities fit into the definition of processing developed by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union (common foreign and security policy in aspects such as law enforcement and borders control). In that case, the Law Enforcement Directive (LED) application in the EU would be of important relevance, with the related safeguards, administrative and public control and oversight of the entities developing such practises.

In any of these scenarios, the development of crowdsourcing that involves the processing of personal data would need to involve important safeguards integrating privacy by design and by default. This integration is of paramount importance for the lawful development of these practices, regardless of the scope of application of GDPR or LED. The advisable privacy by design and by default measures in this case would be the correct development of the data minimisation principle (article 5(1)(c) GDPR), with a correct selection and prioritisation of the sources of information, and the automated anonymisation of personal data.

4.5.5. Processing of personal data with the use of GeoAI systems

Since the inception to the general public of Artificial Intelligence models around the end of year 2022[44], the uses and capabilities of this technology has been improved and explored extensively.

[42] See the investigation of Italy's Data Protection Authority and the preliminary measures that could lead to the blocking of the service in the EU. 'Intelligenza artificiale: il Garante blocca ChatGPT. Raccolta illecita di dati personali. Assenza di sistemi per la verifica dell'eta dei minori' (Garante per la protezione dei dati personali, 31 March 2023) <https:// www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/doc web/9870847#english> accessed 23 February 2025.

[43] Taner Kuru, 'Lawfulness of the mass processing of publicly accessible online data to train large language models' (2024) International Data Privacy Law (advance article) https://doi.org/10.1093/idpl/ipae013 accessed on 23 February 2024.

[44] Date of commercial public launch of access to OpenAI's ChatGPT 3.5 model.

Some of the technologies in which Generative Artificial Intelligence (Gen-AI) are based have been of wider exploration prior to that date, such as machine learning and neural networks. However, the public reach of these technologies has boosted and enabled some uses of these technologies which were not explored before.

Most of the personal data processing investigations and concerns are directed to the use of Generative AI. This technology enables the creation of synthetic data and machine-generated data by automated means. By feeding the models of creation with personal data, it allows to create new data, which can be labelled as synthetic data, but also relatable to an identified or identifiable natural person, fitting the definition of personal data under GDPR. The controversies and potential legal issues around the use of Gen-AI range from the right to object to the processing of personal data, the rectification of inaccurate personal data, the use of deepfakes for identity theft and many others.[45] They will not be analysed furtherly in this report, since this specific development of Artificial Intelligence is of limited impact for the scientific research in project THEIA.

In the future, the inception of Artificial General Intelligence (AGI) is posed to challenge other areas of the right of privacy and the protection of personal data, such as the data minimisation principle, human oversight and the right not to be subject to automated decision making (article 22 GDPR). Since the research in project THEIA does not aim at the achievement or immediate use of this technology, they will not be explored either furtherly in this report.

Geographic artificial intelligence (GeoAI) could be defined as artificial intelligence techniques that leverage the relationships of objects, events and people in geographic space with specific technical, and informational conditions.[46]

[45] Barrio Andrés, Moisés (dir.), Comentarios al Reglamento Europeo de Inteligencia Artificial (1ª ed, La Ley 2024).
[46] Grant McKenzie, Hongyu Zhang, and Sébastien Gambs, 'Privacy and Ethics in GeoAI' in Song Gao, Yingjie Hu, and Wenwen Li (eds), Handbook of Geospatial Artificial Intelligence (1st edn, CRC Press 2023) p. 388 to 405. P. 2

Figure 1. Areas of development of GeoAI. Extracted from "GeoAI Challenge"[47], created by AIforGood

GeoAI as a technology may pose significant risks for the right to privacy of individuals, depending on its use. Some of the already existing legal challenges for the processing of personal data through AI models may be replicated in the use of this technology.[48] The challenges range from different steps in the automated processing of personal data, such as data obtention, data generation, automated decision-making, data analysis, and regulatory oversight. Some authors defend that these issues are not new to the right to privacy as a fundamental right, challenged by technology evolution over time, but rather amplifications and re-combinations of existing privacy concerns.

- Massive Data Collection and data scraping: AI depends on vast amounts of training data, much of which is collected through scraping the internet without consent. This situation and its legal and societal implications are explored in the previous point of this report "4.1.4 Processing of personal data with the use of crowdsourcing and open-source data from social networks". It may well be a legal issue connected with the use of GeoAI, which could exacerbate these problems if the origin of the data is not properly controlled and tracked.

[47] "GeoAI Challenge", created by AIforGood, available at https://aiforgood.itu.int/about-us/geoai-challenge/
[48] List elaborated based on information from Daniel J. Solove, 'Artificial Intelligence and Privacy' (2025) 77 Florida Law Review 1.

- Inference and Data Generation: AI can generate new personal data about individuals based on inference, which people may not expect or want. The implications of synthetic data or newly automatically created data are of limited impact for GeoAI, which does not necessarily rely or interconnect much with Gen-AI.
- Bias and Discrimination in Decision-Making. If a GeoAI model is used to support a decision-making process, and the training of that model is flawed and generating bias against certain groups of population, these biases may pass to those decisions. The risk is particularly bigger if the targeted group include minorities who risk discrimination based on their race, religion, sexual orientation or origin, which may be likely the case when forcibly displaced population are involved.[49] The risk could be greater if decisions are solely based on automated processing, without human oversight. This conduct could breach particularly article 19 GDPR. And against the prohibition of practises related to mass surveillance AI systems contained in article 5(1)(h) of the Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act)[50].
- Surveillance and Identification: AI enhances the ability of entities to engage in mass surveillance and identification, increasing in a significant way risks to personal privacy and autonomy. Techniques like facial recognition and behavioural tracking exacerbate the loss of anonymity. In this sense, see the already described legal framework applicable to automated facial recognition, explained in section (4.1.1 Processing of personal data within the processing of satellite data and UAV/UAS). Especially, the European Data Protection Board Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement.
- Transparency and Accountability Issues. When GeoAI supports the action of border control authorities, or the study on forcibly displaced population, their end-users may be unaware of its design or internal functioning. This is the significant "black box" problem, which generates difficulties in understanding why and how a system works and to understand the outcome of the model. It could potentially generate difficulties to audit, understand, or contest decisions made solely, or with the assistance of this model.

Some authors argue that the current privacy laws were not designed for the scale and complexity of AI. On the other hand, their inapplicability to AI may generate a phenomenon of "AI exceptionalism"[51], where AI's privacy problems are treated as unique and separate from broader

[49] Nicoletti, Leonardo, 'Humans Are Biased. Generative AI Is Even Worse' (Bloomberg, 9 June 2023) https://www.bloomberg.com/graphics/2023-generative-ai-bias/ accessed 24 February 2025.
[50] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence. OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj
[51] Daniel J. Solove (2024), p. 15.

privacy issues. The due combination of compliance to both legal frameworks is the ideal situation, and what the EU regime points in article 2(7) of the AI Act, when establishing the coexistence of Union law on the protection of personal data, privacy and the confidentiality of communications with the AI Act on personal data processed in connection with the rights and obligations laid down thereto.

Some privacy by design and by default solutions are already envisioned in the existing scientific literature regarding GeoAI.[52,53] McKenzie, Zhang, and Gambs[54] discuss the application of data obfuscation and data anonymisation to increase security and privacy in the use of GeoAI. While anonymisation excludes the application of the General Data Protection Regulation, obfuscation is considered a pseudonimisation technique, that retains the category of personal data for the information on which it is applied (see EDPB Guidelines 01/2025 on Pseudonymisation).[55] Some of the methods suggested are network graphs, discrete global grids, and decentralized collaborative machine learning. Synthetic data generation is another method suggested to improve data protection in GeoAI, which may particularly help in the training of the AI models used without the need of private information or personal images. On the other hand, technical capabilities should be evaluated, since the result of this training could be of poorer quality considering the alternatives with authentic personal or industrial data. Cryptography is another well-established method that should integrate the basic toolbox of the use of any AI system and the basis of their telecommunications related to law enforcement.

GeoAI is deeply impacted by the EU AI Act. The complete regulation applies to the use of GeoAI for purposes other than "national security, regardless of the type of entity entrusted by the Member States with carrying out tasks in relation to those competences [... AI systems] used with or without modification exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities." (article 2 AI Act). These activities are outside of the scope of the regulation. However, the fact that these uses of AI are not under the scope of the AI Act, does not mean they are absent to legal scrutiny. The Law Enforcement Directive is still applicable for the processing of personal data within those systems, setting obligations that need to be considered both from private entities and public authorities in the development and use of such services. The current absence of regulation of the use of AI in the military, security and law

[52] Małgorzata Węgrzak, 'Legal Regulations of Artificial Intelligence and the Space Sector: Perspectives and Challenges from the Polish Perspective' (2023) 3 Revista Española de Derecho Aeronáutico y Espacial 45-62.

[53] Giovanni Tricco, 'AI in Outer Space: Reinforcing the Sustainability and Safety of the Low-Earth Orbit in the New Space Era' (2024) 4 Revista Española de Derecho Aeronáutico y Espacial 195-209.

[54] Grant McKenzie, Hongyu Zhang, and Sébastien Gambs, 'Privacy and Ethics in GeoAI' in Song Gao, Yingjie Hu, and Wenwen Li (eds), Handbook of Geospatial Artificial Intelligence (1st edn, CRC Press 2023) p. 388 to 405.

[55] European Data Protection Board Guidelines 01/2025 on Pseudonymisation. Available at https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-012025-pseudonymisation_en .

enforcement domain is a sorry lack of comprehensive regulation, that should be remedied in the future to prevent the abuse of civil liberties and fundamental rights in those areas.

The AI Act underlines important elements of compliance for the space sector. Most of these obligations are applicable to entities operating GeoAI:[56]

- Forbidden practices: AI Operators must prevent the use of the technologies in the situations listed in the AI Act under the label “Prohibited AI practices” under article 5 AI Act. These conducts include the exploits any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person. It also includes the use of an AI system for making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics. This situation may affect forcibly displaced population directly. Any operator should abstain of such practices, if they fall under the scope of the Regulation.
- Classification of AI Systems: AI Operators must determine if their applications fall under the 'high-risk' category, which includes systems impacting critical infrastructure and safety. For instance, AI systems managing satellite operations or space traffic could be deemed high-risk. Although not any GeoAI system should be labelled as high risk just for the fact of being operated in an artificial satellite, or using geospatial data. The assessment must be developed individually for those technologies.
- Compliance Requirements for High-Risk AI Systems: The GeoAI systems that fall under the high- risk category should develop a risk management policy and implement continuous risk assessment and mitigation strategies throughout the AI system's lifecycle. They should also be developed with strict data governance policies that may ensure the quality and integrity of data used, maintaining relevance, representativeness, and accuracy. Their technical details must be maintained with detailed technical documentation and records, demonstrating adherence to AI Act standards.
- Any GeoAI system, regardless of its risk categorisation, should develop transparency and information provision to its users and targets. To the extent possible and balancing this interest with public security and homeland protection, the systems used to enhance Copernicus Security Services capabilities should inform users about the AI system's capabilities, limitations, and intended purposes.

[56] List developed with the information extracted from the following publication, and its adaptation to GeoAI: Węgrzak (2023), see footnote 36.

- Human Oversight: There must always be humans in the loop. Human oversight should be designed and embedded in the organisation in order to establish measures allowing human intervention to prevent or correct adverse outcomes.
- Accuracy, Robustness, and Cybersecurity: Design AI systems to achieve high performance levels and resilience against potential threats.
- AI Literacy and Training: Enhance AI literacy among staff to ensure informed and ethical use of AI systems, as mandated by the AI Act.

The capabilities of GeoAI and the security and respect for the principles protected under the AI Act maybe complemented through data fusion, processing and analysis, based on quantity (multi-temporal data) and variety of data. The development of Machine Learning (ML), data federation and handling of existing and new datasets can be improved with the correct development of crowdsourcing multiple solutions for high-impact problems that could improve real production AI/ML systems.

5. Ethical and social concerns

5.1. General overview

The THEIA project is a scientific research project with the aim of developing technical solutions and boosting tools to enhance Copernicus Security Services and help managing EU governmental crisis related to the forced population displacement. With that goal in mind, a number of technical tools are explored, developed and offered to the testing and access of end-users. In such a development, some ethical issues may emerge considering the deployment of these technologies, which may result invasive for privacy, or affect other fundamental rights. These various interests need to be balanced in the deployment of such technologies. In this initial stage of the research, some of the potential issues are pointed out for awareness and some solutions are offered to improve societal acceptance and reduce the ethical impact of these technologies.

5.2. New technologies: acceptance by the society and trust

5.2.1. Satellite data and UAV/UAS

It is safe to say that the use of artificial satellites is a piece of technology well incorporated in society nowadays. Since the inception of the Space race by the launching of the first satellite Sputnik 1 in 1957, humanity has been launching more and more of these man-made objects to space, with various intentions. They were firstly used to support military operations and for telecommunications. Satellite radio emissions have allowed the communication by humans in remote areas of the world. They are especially used in high seas. Television broadcast has been another one of the areas of artificial satellite communication support. The study of meteorology has also been part of this discipline for many years. The most recent developments are the use of artificial satellites to provide internet connection in any point on Earth, without regards of other technological support.

Currently their use is well established in industrialised countries. There are a total of 7,560 active artificial satellites orbiting Earth[57], operated by a total of 75 countries[58] (including governmental agencies and private companies based on those countries). The societal impact of the use of artificial satellites is currently limited. Some of the implications of this technology have had a certain degree of societal debate, such as the management of Space debris (also known as space junk, space pollution, space waste, space trash, space garbage, or cosmic debris).

[57] Union of Concerned Scientists, 'Satellite Database' (1 May 2023) https://www.ucsusa.org/resources/satellite-database accessed 24 February 2025.

[58] Dewesoft, 'Every Satellite Orbiting Earth and Who Owns Them' (1 September 2021) https://dewesoft.com/blog/every-satellite-orbiting-earth-and-who-owns-them accessed 24 February 2025.

The development in the future of other uses of the available technologies in artificial satellites may be of higher societal impact. From the previously described technologies, some of the imaging may be used in surveillance activities which currently are of limited development due to the tight control of the launch and operation of artificial satellites. However, if the use of those technologies is generalised boundless and without regards of the fundamental rights of people, its use could impact fundamental rights and freedoms at a scale capable to origin societal concerns.

5.2.2. Satellite video and multispectral images

The use of satellite video and multispectral images in the fields of law enforcement could be one of the areas of potential societal concern related to artificial satellites. These technologies have not yet commercially been exploited in a broad sense. They are, in this sense, unknown or of limited knowledge for the general public, since commercial civilian applications for their use are not yet available in the market. Their use could be sensed as justified by civil society if appropriate safeguards are developed for the control of their use in strict circumstances, and in previously designated areas, without the possibility of uniquely identifying individuals, and only for bulk analysis of groups of population. The societal reactions to this use are yet to be seen, and can only be the subject of further analysis as part of the testing of the available tools considering the current state of the art.

5.2.3. Automated detection and identification of objects through satellite video and multispectral images

The use of Automated detection and identification of objects using satellite video and multispectral images could be an area of potential higher societal concern related to artificial satellites. The state of the art regarding these technologies is of wide unawareness for the general public. Therefore, the potential development at a broad global level and implementation of these technologies without individual consent or the due redress legal mechanisms could be of societal concern.

The current state of the art does not allow for the use of Very high-resolution (VHR) optical imaging for automated identification of individuals. This fact, currently underlined and explained while using these technologies, could be of easiness to lower the societal impact and allow for a better implementation of the technologies as the state of the art evolves. The parallel development of civilian oversight on the use of these technologies would be of importance to lower the potential impact and allow for a better and progressive adaptation of the public to the awareness levels and trust.

5.2.4. Crowdsourcing and use of open-source data from social networks

Crowdsourcing and use of open-source data from social networks are in general known only to specialists in the social media industry and digital markets. Most social media users are unaware of the technical details behind how these services operate. Social media platforms typically outline the use of user information and content in their Terms of Service. However, these terms are often complex and difficult for the general public to understand. They rarely mention crowdsourcing explicitly, except when prohibiting data scraping or activities that could harm the platform operator's interests

In general, general consideration of the data that is shared in social media is that it becomes open source, publicly available information the moment it is shared. Some above-average informed users know about the use of public entities of the information shared in social media, and the implications regarding Intellectual Property rights of the sharing of content created through these platforms. If these practices were to be used to enhance law enforcement capabilities, or to manage forcibly displaced population, it would probably pass unnoticed to the general public. Nevertheless, in order for the public to generally accept their use and adequacy to enhance law enforcement, civilian oversight and public auditing would be advisable. Especially for the current explanation of the bypass of privacy regulations in cases of public interest and the applicability of stern safeguards for the anonymisation of the data and the development of privacy by design and by default.

5.2.5. GeoAI systems

The societal acceptance of GeoAI systems will heavily depend on the public awareness of compliance and the benefits foreseen to its use. These benefits will most probably be balanced against other very prosaic and direct effects of the development of Artificial Intelligence: loss of workforce due to the automation of tasks, decrease of human relations due to the improvement of machine-human interaction, loss of privacy due to the increase of machine oriented environments, and so on.

5.3. The necessity to balance fundamental rights and the protection of borders

Fundamental rights such as the ones exposed in section 2. (Prominent legal issues and the protection under the ECHR and the EU Charter of Fundamental Rights) of this report are the backbone of democratic and open market societies. Their respect and impulse are the main, if not the only guarantee that social minorities may live in peace and prosperity in such societies. They form the core of the globalised international relations based in law. Without their presence and respect, only might is right.

Every country has the sovereign liberty to dispose of its own future, its own set of rules and laws that govern its society and guarantee prosperity, peace and conviviality. A main part of this sovereignty is the capability to impose borders and decide on how and when foreigners can reside in its land. When this capability is lost and a country is not able anymore to control its own borders, it loses a main feature in its categorisation as a State. Every country is free to establish these rules, safe with the limits of international law and the respect for fundamental rights.

These two realities must coexist in harmony in the management of borders. Forced population displacement involves millions of people every year. Their fundamental rights as human beings and individuals must be protected, and must be a priority for the international organisations that govern the globalised world. But this priority in the international globalised framework must be developed with responsibility by the public authorities of the States, who have paramount obligations to their own citizens. The objective of the research in THEIA is to help balance both priorities, and to assist EU Member States in navigating the legal problems, ethical difficulties and efficiency checks by improving the use of technology for this goal.

5.4. Liability in case of an ethical or legal breach

Responsibilities of actions within the research activity in project THEIA lay in the party or partner solely and not in the whole consortium. Regarding ethical or legal breaches, liability of such breaches lay uniquely in the partners involved directly in the design of the technology, protocols or decisions affected by the breach. Regarding this topic, the Consortium Agreement[59] establishes in its section 5:

"5.2 Limitations of contractual liability

Each Party shall be solely liable for any loss, damage or injury to third parties resulting from the performance of the said Party's obligations by it or on its behalf under this Consortium Agreement or from its use of Results or Background."

5.5. Main ethical requirements that need to be observed when conducting research

5.5.1. Principles and research methodology

The scientific research in THEIA is bound to respect certain elements and standards to ensure its quality and capacity to deliver balanced results. These elements are based in the project-generated data that can be shared and will be made available as Open Access research data; this refers to the Findable, Accessible, Interoperable and Reusable (FAIR) system, guaranteeing open

[59] THEIA Consortium Agreement p.8.

access and re-use of digital research data under the terms and conditions set out in the THEIA Grant Agreement (section 1.2.11 Research Data Management and Management of other Research Outputs).

THEIA research will also fully comply with Regulation 2021/695 establishing Horizon Europe[60]. Particularly, the provisions about ethics are primarily considered (articles 18 and 19). None of the ineligible activities for funding listed in article 18 are in the scope of project THEIA. About the legal safeguards and principles established in article 19, THEIA has already implemented, or has an established plan to implement all of them. Research in THEIA respects the principle of proportionality, the right to privacy, the right to the protection of personal data, the right to the physical and mental integrity of a person, the right to non-discrimination and the need to ensure protection of the environment and high levels of human health protection. Compliance with these principles is shown in THEIA by:

- The development of an ethics self-assessment, presented in THEIA Grant Agreement[61] and developed in the Ethics deliverable D15.1 OEI – Requirement with further details and compromises to be met in the development of certain reports and research stages.
- Compliance with the European Code of Conduct for Research Integrity published by ALLEA.[62]
- For activities carried out outside the Union, confirmation will be provided that the same activities would have been allowed in a Member State.

Article 20 of the Regulation, on security, is also relevant for THEIA project, as it sets the framework for keeping information in research confidential. Confidentiality and privacy are the main ethical principles that apply to research in the project. Specifically, according to article 20 of the Regulation all:

"actions carried out under the Programme shall comply with the applicable security rules and in particular rules on the protection of classified information against unauthorised disclosure, including compliance with any relevant Union and national law. In the case of research carried out outside the Union using or generating classified information, it shall also be necessary that, in addition to the compliance with those requirements, a security agreement shall have been concluded between the Union and the third country in which the research is to be conducted".[63]

[60] Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013

[61] THEIA Grant Agreement, p. 46 part.B.

[62] European Code of Conduct for Research Integrity of ALLEA (All European Academies).

[63] See Regulation (EU) 2021/695, article 20.

The respect to the principle of proportionality, the principle of non-discrimination, the obtention of informed consent for the processing of personal data, the care for vulnerable subjects are principles imbedded in the THEIA research. These actions develop, amongst others, the right to the protection of personal data, the right to privacy and confidentiality, in order to reduce the potential misuse of research findings for unethical purposes. The right to integrity for the research, and a perspective of the ethical use of incidental findings guide the activity of the partners and the shared research, as well as the processing of geospatial data.

5.5.2. Internal research protocols in THEIA

This section lists a group of ethical rules and principles needs to be observed by all partners who are involved in the THEIA project. This protocol safeguards the rights and freedoms of the research participants, which shall always be respected throughout the research.

I. Principle of proportionality

The form, the means and content of the THEIA research shall not exceed the purpose for which the research is conducted. It shall not exceed the objectives it aims to achieve.

II. Principle of non-discrimination

All human subjects participating in the THEIA research shall be treated equally.

III. Vulnerable subjects

Vulnerable groups of people, including elderly, children, individuals with mental or physical disabilities shall participate in the THEIA research only if this is absolutely necessary for the observation of its purposes. In this case special conditions shall apply to safeguard the rights of these groups of people or individuals. Particularly if they form part of forcibly displaced population, and in regards to the anonymisation of their personal data.

IV. Informed consent

The acquisition of a valid informed consent by the research participants shall be treated as a priority. Whenever possible, and observing strictly the legal impositions on the lawful collection of personal data, informed consent shall be the priority to obtain information from individuals. Whenever required, individuals shall be entitled to withdraw at any stage of the research activities without any implications or penalties. This element will also be observed to individuals participating in the open demos or pilots of the project, as well as individual members of the end-users.

V. The right to the protection of personal data

Any processing activities involving personal data shall be conducted in compliance with the GDPR, EUI-DPR and Law Enforcement Directive. Data subjects shall be informed of the kind of data that are being processed, the purpose of processing, the period of storage, as well as of the possibility

for further transfer of their data to third parties. Special categories of data shall be treated with extra caution, as described in the abovementioned privacy regulations. All rights of the data subjects shall be observed throughout the processing activities. The principle of data minimisation shall apply. Security measures shall be in place to keep the participants data safe from unauthorised access.

VI. The right to privacy & confidentiality

The privacy of research participants shall be respected throughout the THEIA research, complementary to the right to the protection of personal data. Individuals shall keep control over their information as well as over access to them. All parties involved in the THEIA research shall keep any information disclosed to them confidential. Disclosure of such information shall be limited and only developed only for the purposes of the THEIA research and with the prior consent of the research participant to whom the information refers, whenever legally possible.

VII. Potential misuse of research findings

The possibility of misuse of research findings shall be evaluated during the THEIA research, with special attention to the findings that may emerge in the use of GeoAI. In the unlikely event that such misuse occurs, all necessary measures should apply to minimise the risk for the research participants. The Project Coordinator shall always be informed of such incidental findings. The Project Coordinator will evaluate the need to share those findings with the rest of partners of the consortium, and the best course to ensure accountability with third parties and contracting parties to the Grant Agreement. The participants in the THEIA research shall be notified immediately in the event of unexpected incidental findings. Their explicit consent shall be acquired before any such findings are further communicated to third parties.

VIII. Accountability

Researchers participating in the THEIA research shall always be able to demonstrate compliance with the present protocol. In case of violation of any of the above clauses, the THEIA researchers shall be held accountable. Every organisation and partner that participates in the project is liable individually of their own conduct with regards to these protocols.

6. Relevant Regulatory frameworks in specific EU Member States

The development of the research in THEIA amounts for a significant relevance regarding the different EU Member States where it takes place. Specifically, research activities such as case studies, demo activities and pilots will be organised in specific locations. The different national legal framework regarding the subject of THEIA research may require the adaptation of such activities, and the research in the project, to such extremes. This is of particular relevance when the privacy and data protection framework is analysed. Slight differences between the regulation in different Member States may amount to accumulated divergence at the end of the project, if these differences are not analysed properly.

At the current stage of the research, it would be of limited interest to analyse the national legal framework applicable for the research. Premature disclosure of such information may hinder the development of case studies, demos activities and pilots in the project. The applicable legal framework will be analysed when the location and content of such activities are defined, and if such disclosure is compatible with the public nature of the reports in Ethics in project THEIA.

7. Collection of consent for the processing of personal data

7.1. Informed consent with regards to processing of personal data for participants of THEIA activities.

The development of the THEIA research activities will involve the organising of case studies, demo activities and pilots where the different technical elements developed in the project will be tested. These activities will entail the engagement with external entities to the research and third parties.

Deliverable D3.1 THEIA Ethics version 1 (1st period) (M3) is a report on ethical and legal aspects of the project. Among other elements, it includes some template consent forms in the content of this deliverable. The consent forms are the appropriate way to collect consent for the processing of personal data in these open activities, fulfilling, when necessary, the controls set in articles 6(1)(a), article 7 GDPR. The consent forms were elaborated considering the established administrative guidance set in the EDPB Guidelines 05/2020 on consent under GDPR[64] handed to the participants in the demo activities in case that their personal information is collected, in order to obtain their valid consent to process their personal data. This is a general practice in this type of research projects in which demo activities and pilots based on use cases are developed.

Considering that these open research activities form part of task T12.1 (Definition of application use cases and demo activities requirements), which will only be initiated from M15 onwards, there are not sufficient details at this stage of the research to properly define the scope of the activities. However, in the spirit of boosting transparency and accelerating the process of legal compliance, a first of the template consent forms is offered in this report as Annex I.

The templates are created with a number of assumptions in mind. The first assumption is that the main engagement during the demo activities will be between the members of the consortium and the end users. The end users' members will express their interest in the technology that we are developing, and they will collaborate with the THEIA consortium members in testing it on the ground. End users will need to agree to participate in the pilot. For that, and in the event that their members' personal information is collected, the consent forms will be used. The second assumption is that there will not be any participation of external subjects in the tests. In the event of external engagement that implies people under surveillance using THEIA's technology, their data will be anonymised, therefore, there will be no need to collect their consent for the treatment of information.

If any of these assumptions need to be re-evaluated when the development of the research allows for a better planning of the open activities, the template for the consent forms will also

[64] European Data Protection Board Guidelines 05/2020 on consent under Regulation 2016/679. Available at https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

be adjusted, and the final version, as well as the filled-up forms themselves will be attached to an Ethics deliverable in the future versions and iterations of Work Packages 3 and 4.

7.2. Elements of the Information Sheet on Data Processing

The elements listed below will be included in the information administered to potential participants of THEIA pilots, demo activities and use cases. It is the task of each partner responsible for the organisation of the activities to tailor this information to the points or elements listed below to the concrete circumstances and capacities of the person concerned.

1. An overall description of the THEIA project (including information about the financing of the project and possible conflicts of interest);
2. An overall description in a comprehensive manner of THEIA system's architecture;
3. The description of THEIA's pilots, demo activity or use case where the data subject participates (date, place, aims, activities and tools applies in activity, participating partners);
4. Types of personal data to be processed;
5. Purpose(s) of data processing;
6. The method(s) and tool (s) of collecting data, including any means of automated decision-making, including profiling;
7. An overall description of processing activities;
8. The list of entities involved in processing of personal data:

   8a. Type of entity [project partner/external entity]

   8b. Processing status [data controller/data processor]

   8c. Name of the entity and contact detail (including Data Protection Officer's details when applicable)

   8d. Processing activities of the entity
9. The free and voluntary nature of the participation and consent;
10. The possibility to withdrawn the consent at any time without consequences;
11. Type and extent of data collected and purpose of collection;
12. Confidentiality of data collected: how/where/for how long it will be stored; security measures in place, who will have access;
13. Expected duration of data processing and storage;

14. The opportunity to have any supplied personal data destroyed on request (unless such a request would render impossible or seriously impair the achievement of the objective of that processing – including the impairment or invalidation of the research);
15. The name and contact details of the person(s) responsible for the data collection and processing, including the Data Protection Officer, if applicable;
16. The regulatory authority for the territory of the processing activities;
17. All other rights of the participant conferred by the GDPR (Articles 15 to 21 GDPR) as set out in the informed consent form above.

ANNEX I

Template for consent forms (v1)

Form of the informed consent with regard to processing of personal data for participants of THEIA activities

I, undersigned [**name**] [**date and place of birth – natural person**] [**contact details**], hereby give my consent to the processing of my personal data carried out by the THEIA Consortium with regard to my participation in its pilot/ demo activity / use case [**name**] for the purpose of this research project.

1. I have been informed that the THEIA project (Enhancing Copernicus Security Services - EU governmental crisis management hub for forced population displacement) is a research project currently run under the Horizon Europe Framework Programme under the grant agreement no. 101190051. The coordinator of the project is Geosystems Hellas It Kai Efarmogesgeopliroforiakon Systimaton Anonimietaireia (GSH), whose representative is [**name and email**] who might be contacted with regard to any question regarding my participation.

2. I have been informed about the nature and the purposes of the project, including the duration and the possible risks and benefits of participation. I have read and understood the Information Sheet dated [**DD/MM/YYYY**], or it has been read to me. I have had all my questions answered to my satisfaction.

3. I understand that my participation in the research will include [**describe briefly**] as set out in the Information Sheet dated [**DD/MM/YY**].

4. I understand that personal data about me will be collected and processed on the basis of my consent and that it will be treated confidentially. I understand that the information obtained during the research will be used for the specific purpose of this research project, as set out in the Information Sheet dated [**DD/MM/YY**].

5. [In case the THEIA system uses any form of automated decision-making, including profiling, please include here].

6. I have been informed that my personal data collected during the research will be pseudonymised to the highest extent possible, i.e. all possible efforts will be made to prevent the identification and attribution of the personal data to myself.

7. I agree to my personal data being processed in the way as explained to me and set out in this consent form as well as the Information Sheet dated [**DD/MM/YY**].

8. I have been informed that the data controller(s) in the pilot I participate is/are [**partner(s)**] [**contact details**] and that I can contact them [or their Data Protection Officer [**name & contact details**]] to ask questions and exercise my rights.

9. I have been informed of my rights related to the use of my personal data in line with the General Data Protection Regulation (Regulation (EU) 2016/679) and relevant national law, including:

(i) that I have the right to ask the data collector what data are being collected about me and how those data will be used in connection with the trial ("right to access") and that I have a right to lodge a complaint with a supervisory authority;

(ii) that I have the right to request the data controller to correct any of my personal data that are inaccurate ("right to rectification");

(iii) that I have the right to request the data controller to erase my personal data ("right to erasure" also "right to be forgotten"), unless such a request would render impossible or seriously impair the achievement of the objective of that processing – including the impairment or invalidation of the research;

(iv) that I have the right to request the data controller to restrict the processing of my personal data in case ("right to restriction of processing");

(v) that I have the right to receive the personal data related to me which I have provided to the data controller and to transmit those data to another controller ("right to portability"); and

(vi) that I have the right to object, at any time, to the data controller regarding the processing of my personal data ("right to object").

10. I am informed that no further use of my personal information in the course of the project is foreseen. I understand that any further use of my personal information will require my separate consent.

11. I give this consent fully informed, freely and voluntarily and I understand that I am free to withdraw it.

12. I have been informed that the Data Protection Authority in [**country**] is the [**name national DPA**], who I have the right to submit a complaint to.

13. The relevant laws of [**country**] shall apply.

Done in two copies, of which one is for the THEIA Consortium and one for the participant.

Name of the participant: _____

Place / date: _____

Signature: _____

[END OF THE FORM]

Informed consent form for participation in research

I, undersigned, hereby give my consent to take part in the reserach related to the pilot/ demo activity / use case in [city, location] (COUNTRY name) organised by the THEIA Consortium.

1. I have been informed that the THEIA project (Enhancing Copernicus Security Services - EU governmental crisis management hub for forced population displacement) is a research project currently run under the Horizon Europe Framework Programme under the grant agreement no. 101190051. The coordinator of the project is Geosystems Hellas It Kai Efarmogesgeopliroforiakon Systimaton Anonimietaireia (GSH), whose representative is [name and email] who might be contacted with regard to any question regarding my participation.

2. I have been informed about the nature and the purposes of the project, including the duration and the possible risks and benefits of participation. I have read and understood the Information Sheet dated [**DD/MM/YYYY**], or it has been read to me. I have had all my questions answered to my satisfaction.

3. I understand that my participation in the research will include all the activities of this pilot as set out in the Information Sheet dated [**DD/MM/YYYY**].

4. I understand [**I will/ will not**] be paid for my participation.

5. I give this consent fully informed, freely and voluntarily and I understand that I am free to withdraw my consent and discontinue my participation at any time without any negative consequences.

6. The relevant laws of [**COUNTRY name**] shall apply.

Done in two copies, of which one is for the THEIA Consortium and one for the participant.

Name of the participant: _____

Place / date: _____

Signature: _____

END OF DOCUMENT