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

D3.2 THEIA Ethics version 2 (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	Javier López-Guzmán (MPL)
Reviewers	Sven Schlarb, Ines Burgstaller (AIT)

Due Date	28/02/2026
Delivery Date	28/02/2026
Type	ETHICS
Dissemination Level	PU - Public
Keywords	Ethics, questionnaires, ethics by design

Document History

Version	Date	Description	Author	Description/Action	Validation
0.1	31/12/2025	Outline & Table of contents	Javier López-Guzmán (MPL)	Initial overview of the deliverable structure	
0.2	01/02/2025	First draft	Javier López-Guzmán (MPL) Vagelis Papakonstantinou (MPL)	First draft of the updated document	
0.3	19/02/2025	First internal version	Javier López-Guzmán (MPL) Vagelis Papakonstantinou (MPL)	Request for partners' input	Consortium partners' comments collected and incorporated.
0.4	20/02/2025	Revised version	Sven Schlarb, Ines Burgstaller (AIT)	Inclusion of partners' comments	
0.5	23/02/2025	Second internal version	Javier López-Guzmán (MPL) Vagelis Papakonstantinou (MPL)	Revised version	SATCEN review completed. Feedback incorporated.
0.6	25/02/2026	Final Draft	Francisco Javier López Guzmán (MPL) Vagelis Papakonstantinou (MPL)	Finalisation and approval	SAB security check completed. Feedback incorporated. into the document.

1.0	27/02/2026	Final version	Liza Panagiotopoulou (GSH)	Submission to EC	
1.1	26/03/2026	Updated Final version	L. Panagiotopoulou (GSH)	Inclusion of missing inputs from C3I	
1.1	31/03/2026	Updated Final version	L. Panagiotopoulou (GSH)	Submission to EC	

Legal Disclaimer

Contents

Executive Summary

The current deliverable, D3.2 “THEIA Ethics version 2 (1st period)”, corresponds to Task T3.1 – “1st period project ethics and legal aspects of THEIA” under WP3 – “Ethics 1 - 1st period”, led by MP Legal.

This report serves as the third iteration on Ethics in the project. It follows deliverable D15.1 OEI - Requirement No.1, which consisted on a self-assessment on Ethics prior to the beginning of the research in the project (completed in M1). And, it also follows Deliverable D3.1 “THEIA Ethics version 1 (1st period)”, a regulatory benchmark analysis on Ethics, and the development of consent forms for the pilots, open demos and use cases in the project (completed in M3). The analysis on Ethics will be continued during the rest of the duration of the project, and will have a following iteration in WP4 – “Ethics 2 – 2nd period” at the very end of the project.

The current deliverable contains an assessment on Ethics based on self-reporting questionnaires completed by the partners in the project. It touches upon specific topics with Ethical relevance emerged from these questionnaires, and reflects on the efforts on Ethics by design integrated in the project. Amongst other topics, a Data Protection Officer assessment and Data Protection Impact Assessment evaluation of pertinence are developed, together with an analysis on specific ethics aspects of the UAS and terrestrial sensor-based image processing, the potential risks of eavesdropping related to radio-frequency data, the crowdsourcing information analysis and a demographic data analysis.

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
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
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.
IR	Infrared
LEA	Law Enforcement Agency
LED	Law Enforcement Directive
ML	Machine Learning
NDA	Non-Disclosure Agreement
ParDPO	Partners’ Data Protection Officers
UAV	Unmanned Aerial Vehicles
UDHR	Universal Declaration of Human Rights
UAS	Unmanned Aerial Systems
UN	United Nations
OSINT	Open Source Intelligence
RF	Radio Frequency
RGB	Red Green Blue
SIGINT	Signals Intelligence
WP	Work Package

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 second 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 (M3-M15). Ethics, data protection and privacy are covered in a complete 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 an overall analysis of the research in the project from the ethics perspective. It integrates the responses of the partners to the Ethics questionnaire, selected analysis on specific ethics aspects such as the crowdsourcing information, RF signals and the risks of eavesdropping, RGB data and thermal signals collected through ground sensors, and other horizontal ethics aspects such as the DPO and DPIA necessity evaluation, the responsibilities of the Ethics Manager, and the role of the Ethics Advisor.

This document is to be read in conjunction with the Data Management Plan included in Deliverable D1.5 "Intermediate Data Management Plan (DMP)". The information completed in both reports is complementary in specific sections.

1.1 Purpose and scope of the deliverable

The purpose of the deliverable is to develop ethics compliance, describe the personal data processing in the project and other ethics aspects about the research.

The report covers the following aspects:

- Ethics questionnaire; engagement with the partners of the consortium as a first step for the development of privacy by design and by default.
- Selected analysis on specific ethics aspects such as:
    - The crowdsourcing information, and the impacts on the right to privacy of the processing of publicly available and open-source data.
    - RF signals and the risks of eavesdropping, the analysis of the main types of data collected and analysed in the datasets.
    - RGB data and thermal signals collected through ground sensors, and their potential anonymised use.
    - The evaluation of the necessity of a Data Protection Officer for the project.
    - The evaluation of the necessity of a Data Protection Impact Assessment.
    - The responsibilities of the Ethics Manager, and the role of the Ethics Advisor.

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 includes the instructions of the Ethics questionnaire and its methodology.

- **Chapter 3** includes an overview of the categories of questions in the questionnaire.
- **Chapter 4** includes the instructions to locate the answers to the questionnaire by the partners.
- **Chapter 5** includes the aggregate statistics about the responses to the questionnaire, and the commentary on selected ethics aspects derived from the responses.
- **Chapter 6** includes an overview of the Ethics by design developments in project THEIA.
- **Chapter 7** includes the role and responsibilities of the Ethics Advisor.

- **Annex I** Terms of reference Ethics advisor
- **Annex II** Partners' responses to the Ethics Questionnaire

1.3 References

- Project GA with No. 101190051
- 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
- Horizon Europe Programme Guide, version 5.1 (2025) https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/programme-guide_horizon_en.pdf
- D3.1 - THEIA Ethics version 1 (1st period).
- D1.3 - Initial Data Management Plan (DMP).
- D1.5 – Intermediate Data Management Plan (DMP).

2. Methodology: instructions to respond to the questionnaire

This report, Deliverable D3.1 "THEIA Ethics version 2 (1st period)", is the third iteration with WP3-Ethics 1 – 1st period. This Work Package develops the ethics overview of the research in project THEIA. It is an assessment of the main elements in the project regarding ethics, data protection, and privacy. It exposes the most important compliance elements in project THEIA, and it integrates the legal research and ethics within the project development. It comprises the partners activity that ensures the preparation of legal documentation within the project. It develops the privacy and ethics approvals for each pilot in the project. This WP had two previous outputs:

1. OEI - Requirement No.1. It developed an Ethics self-assessment, prior to the start of the research in the project. It was due in month M1 of the project.
2. Deliverable D3.1 "THEIA Ethics version 1 (1st period)". It showed a benchmark legal analysis of existing applicable legislation to the research in the project. It included a set of Consent forms to be used in the project pilots, demonstration activities and use cases. It was due in month M3.

The present report collects the output of the research in the project regarding ethics during the whole first period of the research (M1 to M15). It is based on a compliance analysis to integrate ethics by design in the project. It is based in a self-reporting methodology using questionnaires.

The ethics questionnaires were elaborated by MP Legal, as lead beneficiary in WP3, and reviewed by WTOC and GSH, the partners with active involvement in this WP. The questionnaires consisted on a survey based on a total of 77 questions on ethics matters. It was circulated to the partners on 4th December 2025, for their assessment and completion.

The questionnaire was sent with a guidance note developed by the Ethics manager, as well as specific instructions for its completion elaborated by MP Legal researchers. It was created using an interactive online platform, Qualtrics[1]. The platform was used as a tool to collect the responses of the partners. All of the questions were in a multiple choice format, or requiring a limited written input. The access to the questionnaire was offered to the partners via an online link,

[1] https://www.qualtrics.com/

protected with an access password. All the partners in the project participated in the survey and responded to the questionnaire. Only one response per partner was required.

The responses of the questionnaire were used by the partners with active involvement in WP3 to integrate an ethics by design approach in the project. Prior to the circulation of the questionnaire, a consultation round was completed with the rest of the partners to collect information that would help design the questions. The partners were offered feedback on their responses on individual basis when relevant information about ethics was found, as well as indications on how to integrate ethics by design.

3. Specific questions

This section specifically covers the structure of the questionnaires. It does not reproduce the literal content of the questionnaires. For the reference of the exact formulation of the questions, it is possible to consult the direct partners' responses at the end of this report as Annex II. The questionnaire was divided into 10 sections, each one of them corresponding to a specific aspect of the project research.

3.1 Organisation details

This chapter summarises the biographical information of the respondent, referring to their category, as project partners, end users, or stakeholders. The respondents are identified as members of one of the project partners organisations. They are asked to state their name for the purpose of contact to integrate ethics by design and obtain feedback on their answers. Their names are redacted in the annexes of this report.

3.2 Questions related to the technology

This second section of the questionnaire relates to the description of the technology. The respondents are requested to describe and define the technical tools that they are developing in the project, and the objectives fulfilled, or to be fulfilled, with its development.

3.3 Questions related to the protection of personal data

The third chapter of the questionnaire pertains to the processing of personal data. The project partners are requested to state if they have processed, or intend to process in the future, any personal data within the development of these technical tools. The partners are required to describe the sources of the data, which data categories they are processing, the information provided and requested from the data subjects, the purposes of the processing, the necessity evaluation of the processing, the storage of the data, their recipients, a mention to the retention period of the data, the potential anonymisation, pseudonymisation, and other privacy by design and by default measures. All this information gathers an assessment of the main elements of

personal data processing under the EU General Data Protection Regulation[2] and the EU Institutions Data Protection Regulation[3] (EUI-DPR).

3.4 Questions related to the datasets

The fourth section of the survey includes questions on the aggregated datasets used in the project. They generally refer to any dataset, including or not personal data. They describe the origin, sources and potential inclusion of personal data in them. This information is to be completed and read in conjunction with the Data Management Plan included in Deliverable D1.5 "Intermediate Data Management Plan (DMP)".

3.5 Questions related to privacy

Section 5 develops a general assessment of the right to privacy in the project. Its protection, respect and impact during the project lifecycle, the impact of the processing of personal data on the right to privacy of the individuals affected, and the adequacy and necessity assessment of such processing, with a balance between the individual rights affected, and the benefit of the potential privacy impact. It also questions the impact of the research over moral, religious or cultural integrity of individuals.

3.6 Societal benefits and risks

This section develops on the potential benefits obtained by the use of the technology. It also informs about the potential risks or ethical issues derived from their use.

3.7 Misuse of research data

The potential misuse of research data is referred in section 7 of the questionnaire. It pertains to the unlawful access, use or processing of data collected in the research for different purposes than the original.

3.8 Risk of stigmatisation or discrimination

The potential risks of stigmatisation or discrimination are described in section 8 of the questionnaire. This element is of special relevance in project THEIA, being the scope of the research the potential development of technical tools for end users to be deployed in border areas for the monitoring and surveillance of such spaces, with minorities potentially affected who

[2] 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.

[3] 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.

risk discrimination based on their race, religion, sexual orientation or origin. These situations may unfold if forcibly displaced population are involved.

3.9 Gender equality

The ninth section of the questionnaire asks the partners to describe potential amplification or generation of gender bias through the use of the technical tools developed in the project.

3.10 Final remarks

The final section of the questionnaire suggests raising certain topics which may have been overseen, skipped or not properly addressed in the design of the questions.

4. Answers of partners to the questionnaires

The answers of THEIA partners to the Ethics questionnaire are included in this report as Annex 2. They are listed as such, partner per partner, without any edition, and as provided by the researcher or member of the consortium who developed the answers. One minor redaction has been developed by MP Legal: the elimination of the name of the researcher. This name was required as a contact point to develop ethics by design and by default measures. The names have been redacted in the questionnaire to safeguard the identity of the researchers involved in the project.

5. Aggregate results of the questionnaires and ethics analysis

5.1 Aggregated results

The Ethics questionnaires are addressed to the partners in project THEIA to assess specific aspects about the development of the scientific research, including the respect to the right to privacy and data protection, the prevention of bias, the risk of discrimination, and other ethical impacts. This section shows some of the aggregated results of interest, presented for overall analysis. All the partners in the project participated in the survey and responded to the questionnaire. Only one response per partner was required. AIT researchers completed the questionnaire in various responses, due to the incidental finding of relevant information between the first and second responses. ICCS responded twice to the questionnaire, due to a coordination error between the researchers team. CREOTECH also responded twice to the questionnaire, due to similar coordination mistakes inside the researchers team, with different responses related to different technical developments within the project. GSH was in a similar situation, but their duplicate responses were not added, since they were integrated in only one response later in time. The rest of duplicate responses are registered in this deliverable, which are nonetheless complementary and do not include any contradictions. There was another response extra due to a technical glitch in the questionnaire that is not reproduced in this report, because is totally vacant. It does not include any relevant information. C3I produced a first response to the questionnaire with erroneous answers, outside of the scope of the project, due to a material error. After they were requested to re-submit their responses, a second questionnaire response was generated by them, untimely. Therefore, a new version of this deliverable was submitted after its due date, to include their full response after a careful assessment. Some of these aspects will undergo an internal ethics evaluation, and will be included in the next iteration of WP4 on Ethics. This should be noted in the responses, as there are only 12 partners in the project, but the overall statistics include 18 responses, for these reasons.

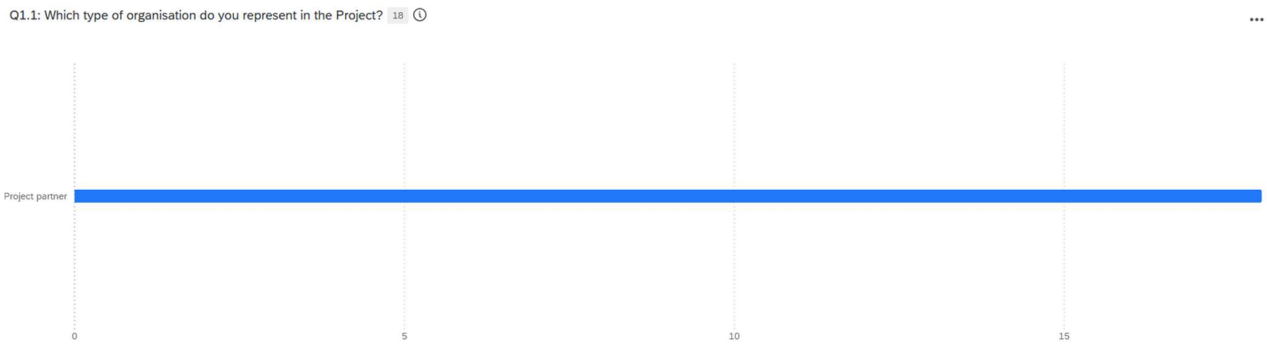

Figure 1. Aggregated results: type of organisation in the project

18 responses to the questionnaire were registered, all presented by project partners. The questionnaires were elaborated to potentially be presented also to end-users and other stakeholders. However, at this point in the research of project THEIA, only the involvement of the partners was required.

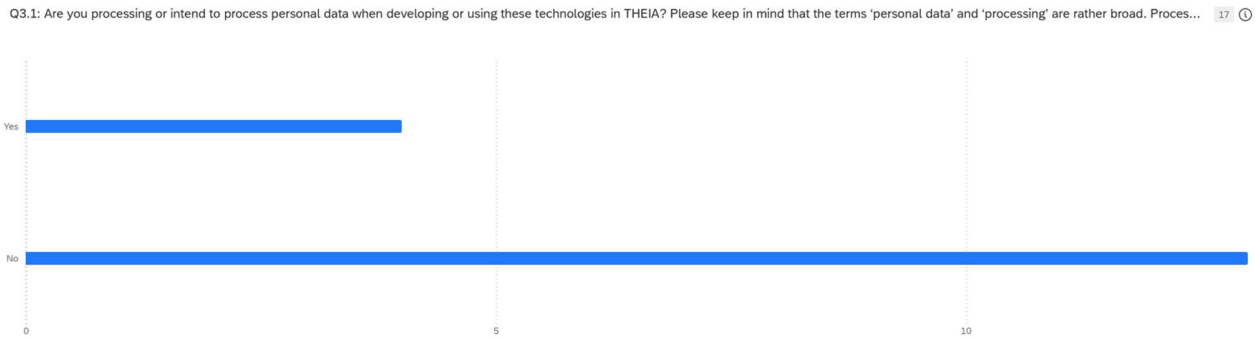

Figure 2. Aggregated results: do you process personal data?

13 responses from the partners stated in their self-assessment that they do not process any information related or relatable to individuals that may qualify as personal data. 4 of them affirm that they do process some personal information.

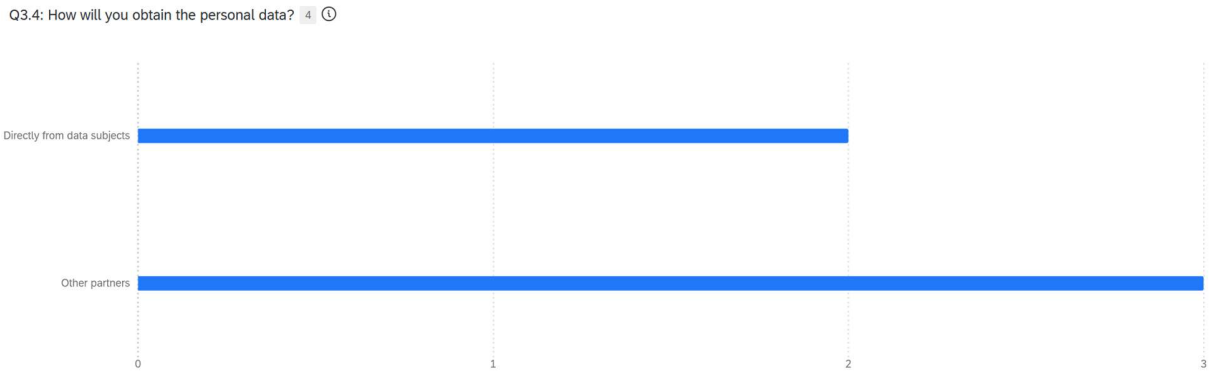

Figure 3. Aggregated results: sources of the personal data

The sources of the personal data in project THEIA are purely internal. Either a direct access via the data subjects, or through the standing collaboration between the project partners.

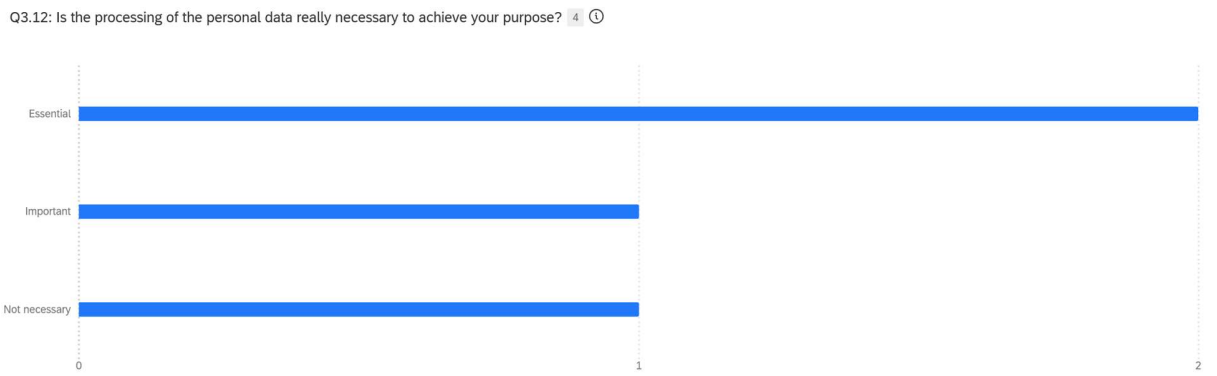

Figure 4. Aggregated results: necessity of the processing

Most of the processing of the personal data in project THEIA is essential or important for the objectives of the research in the project.

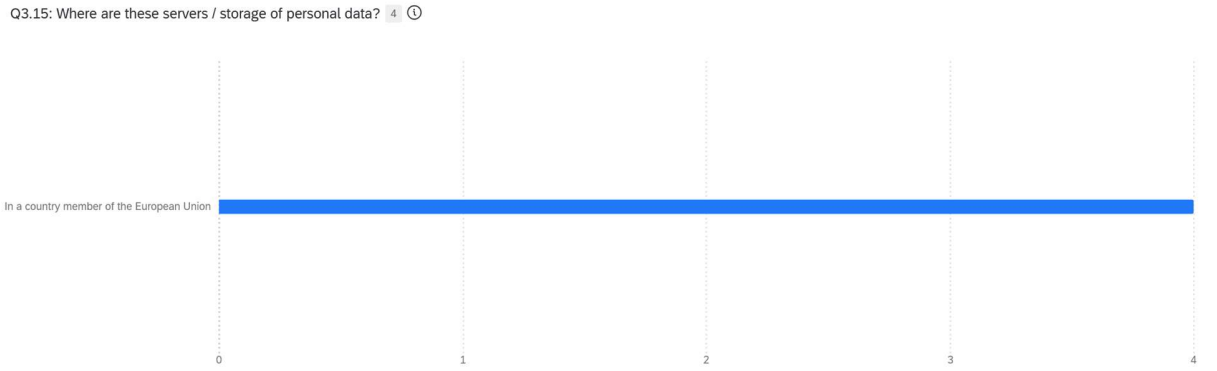

Figure 5. Aggregated results: storage and international transfers

All the partners in the project declare that they store the data in servers or cloud services based in the EU territory. International transfers of the personal data are, therefore, excluded.

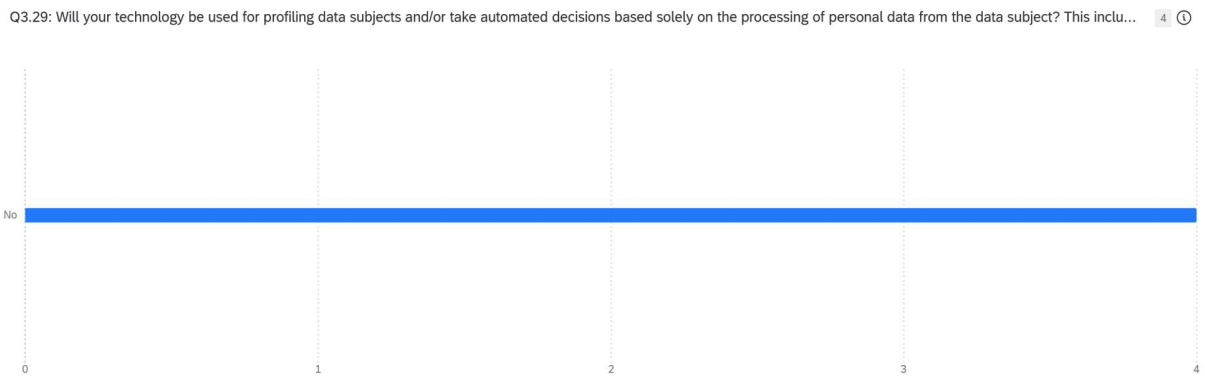

Figure 6. Aggregated results: profiling

Personal data in project THEIA is not used for profiling. Automated decision making over individuals is explicitly excluded from the scope of the project.

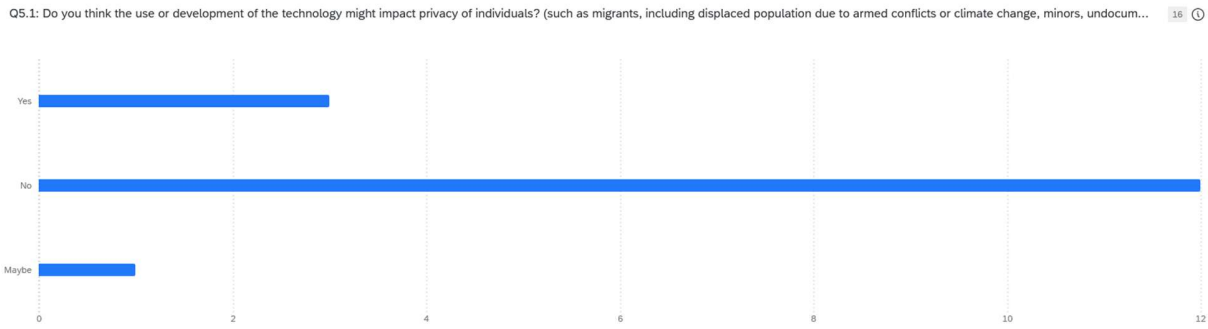

Figure 7. Aggregated results: privacy

Most of the partners in the project consider that the technological developments in project THEIA will not affect the right to privacy of individuals.

5.2 Commentary on specific ethics, privacy and data protection aspects

5.2.1 Data Protection Officer assessment

The EU General Data Protection Regulation of the European Union mandates the appointment of a Data Protection Officer (DPO) for certain entities. Under article 37 GDPR, if an undertaking processes personal data, and is immersed in one of these situations:

a) It is considered a public authority or body, except for courts acting in their judicial capacity;
b) Develops processing operations which qualify for a regular and systematic monitoring of data subjects on a large scale, as its core activities;
c) Processes special categories of data on a large scale pursuant to Article 9, and personal data relating to criminal convictions and offences referred to in Article 10.

In these circumstances, the undertaking must appoint a Data Protection Officer. The DPO is a legally mandated, independent compliance officer designated by certain controllers and processors under privacy regulations, entrusted with advisory, monitoring, and liaison functions to ensure effective compliance with EU data protection law. It is considered by the European Data Protection Board as "*a key player in the [...] data governance system*"[4].

None of these circumstances appear in project THEIA research. The consortium members do not develop any operation which could qualify as a regular and systematic monitoring of data subjects on a large scale in the scope of the project. Neither do they process special categories of data on a large scale in the project research. Therefore, none of the partners in the project are obliged to appoint a DPO for the duration of the project. The project consortium as an entity does not have legal personality, and does not process personal data in aggregation, as a unique entity. Therefore, it is decided not to appoint a THEIA DPO.

Some of the partners have effectively appointed a DPO, considering their activities outside of the scope of THEIA project, or as a qualified and voluntary regulatory compliance measure. Amongst them, there are public entities, mandated to have a DPO under article 37 GDPR, or articles 43 to 45 of Regulation 2018/1725 (EU Institutions Data Protection Regulation). The appointments and contacts are referenced in section 2.4.3 Data Governance of THEIA of deliverable D1.5 "Intermediate Data Management Plan DMP" as partners' DPOs (ParDPO). For those partners without a DPO, a data protection responsible contact is established.

5.2.2 UAS and terrestrial sensor-based image processing

The research in project THEIA includes the technical development of Unmanned Aerial Systems (UAS). It also includes the development of terrestrial sensors for the detection and tracking of

[4] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Officers ('DPOs')' <https://ec.europa.eu/newsroom/article29/items/612048>. P. 5.

specific areas. These developments are created and tested as part of the research in work packages WP7 – Micro-satellite Cubesats and UAS-based data acquisition, and WP10 – Geospatial Artificial Intelligence (GeoAI) and Machine Learning. The testing of these sensors of the ground-based multi-sensor platform involves the potential processing of personal data. These sensors capture video feed through cameras integrated in a multi-sensor platform that record RGB and infrared (IR) data. These recordings involve individuals, who show in the video feed, in order to test the sensors, develop/evaluate algorithms, and process the data in the multi-sensor platform. Individuals engage voluntarily in the project. They are offered information about the project and about the processing of these recordings. Their consent for the processing of personal data is obtained through consent forms. This process is managed by AIT, the partner who develops the terrestrial sensor-based image processing, and the UAV data processing is developed by C3I. The consent may be revoked and the data supressed from processing. The processing, storage and elimination of the data are described in the responses to the questionnaires in annex to this report.

To this point in the research only anonymised data has been used in the scope of THEIA project research (video-feed images where individuals cannot be identified). These data are excluded from the definition of personal data under article 4 section 1 of the EU General Data Protection Regulation, since they are not "relating to an identified or identifiable natural person ('data subject')". This assessment follows the European Data Protection Board (EDPB) instructions and indications in its Guidelines 3/2019 on processing of personal data through video devices[5]. In paragraph 8 of the Guidelines, the EDPB explicitly recognises that certain video-feed data may not constitute personal data: "*the Regulation does not apply to processing of data that has no reference to a person, e.g. if an individual cannot be identified, directly or indirectly.*" It also aligns with the doctrine established by the European Court of Justice in cases C-413/23 P (SRB vs EDPS)[6] and C-319/22 (Scania)[7]. The Court has maintained through its jurisprudence that information obtained as personal data may not be considered as such if the controller or processor does not have access to the identifiers which allow to trace the identity of the data subject. Therefore, in

[5] European Data Protection Board, 'Guidelines 3/2019 on Processing of Personal Data through Video Devices' (2020) https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en .

[6] *Case C-413/23 P: European Data Protection Supervisor v Single Resolution Board (EDPS v SRB)* [2025] Court of Justice of the EU, ECLI:EU:C:2025:645.

[7] *Case C-319/22: Gesamtverband Autoteile-Handel eV v Scania CV AB* [2023] Court of Justice of the EU, ECLI:EU:C:2023:837.

application of this doctrine, the information processed so far in relation to the RGB data in project THEIA may be considered anonymised[8,9].

In future developments of the research, privacy by design and by default measures will be encouraged, such as the automatic blurring of faces to obscure the video-feed and impede the identification of individuals, as well as data minimisations developments. Infrared signals do not allow the identification of individuals, as they only record the heat signature, which is not to be considered personal data, unless associated with other information that may complete the identification of the person. More details about this processing are offered in Deliverables D3.7 Assessment of UAS and Terrestrial Sensing (section 4.2 Data Acquisition), and Deliverable D1.5 "Intermediate Data Management Plan (DMP)", and will be offered in further iterations in work package WP4 Ethics 2 - 2nd period, and the implementation of the work within task T10.2 UAS and terrestrial sensor-based image processing and georeferencing.

These details do not bind to the further use of the technologies developed by end users. The final users of the technology may need to comply with other laws, at European level (e.g. Law Enforcement Directive[10]) or national level. The development of the research in the project does not preclude the potential need for further development of privacy by design and by default measures in the deployment of the UAS and terrestrial sensor-based image processing tools. It neither precludes the potential need to develop a Data Protection Impact Assessment for the use and effective deployment of the systems by the end users.

5.2.3 Risk of eavesdropping and communications interception on RF data

Within the scope of project THEIA, certain technical capabilities around signals intelligence (SIGINT) are developed. SIGINT is the collection and analysis of information transmitted via

[8] Natalia González, Danielle Borges and Marco Botta, 'International Transfers of Personal v. Non-Personal Data: Reconstructing the EU Legal Puzzle' [2026] International Journal of Digital Law and Governance.

[9] Douwe Korff, 'The Concepts of "Data Subject", "Personal Data", "Pseudonymous Data" and "Anonymous Data" in the EU GDPR' (Social Science Research Network, 11 November 2025) <https://papers.ssrn.com/abstract=5734864> accessed 18 February 2026.

[10] 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.

electronic emissions, like radars and telecommunications systems. Amongst others, Radio frequency (RF) technologies are of particular relevance for THEIA scope.

These signals, collected, processed, and interpreted correctly, may provide intelligence information, and constitute SIGINT. They may be of potential relevance for law enforcement agencies and public entities in the safeguard of borders, and provision of rescue missions for displaced population in border areas. Project THEIA intends to develop technical capabilities that enable the integration of SIGINT, particularly RF signals, into a single platform (THEIA platform) with other relevant data and information, to be provided to end-users in for their assessment and control.

Within this development in project THEIA, in the current scope of the research, there is not any processing of information through these signals that qualifies as personal data under the General Data Protection Regulation or Regulation 2018/1725 (EUI-DPR). Different datasets including RF data and Earth Observation (EO) information are processed in the scope of the project (as described in Deliverable D1.5 “Intermediate Data Management Plan” and D7.1 “Assessment of current and planned EO (Optical & SAR) micro and pico-satellites and RF satellites mission”).

Nevertheless, the scope of use of this information in project THEIA is strictly delimited. RF data and analytics are limited to RF geolocation parameters (including timestamp, accuracy level and, if feasible, fingerprint as well). The fingerprint is an unique signal characteristic of navigation radars which is derived from signal processing of emitted RF signal. The data acquired in the project from RF should only contain geolocation and timestamps. As per User Requirement #1 (USR01) in deliverable D5.1 “Stakeholders engagement plan, CSS Gap Analysis Report and User Feedback Summary”: “the system receives only the RF detection signal (including timestamp and location) and not caption of transmitted messages”. Caption of transmitted messages through radiofrequency are explicitly excluded. With that exclusion, the signals mentioned do not qualify as personal data, under article 4 section 1 of the EU General Data Protection Regulation (see previous section of this report, 5.2.2 UAS and terrestrial sensor-based image processing, for a comprehensive legal analysis on the doctrinal application of this legal precept).

THEIA platform is designed to receive and process strictly these types of information through RF. All the agreements for RF data acquisition established with any of the available RF providers stipulate the respect for individual privacy. These agreements do not qualify as Data Processing

Agreements[11], since their content do not list obligations and instructions between data controllers and processors. However, they are agreements for the relation between providers and controllers of the data, in which personal data are explicitly excluded from the datasets. They are limited to the data necessary for the operational needs in the project.

Some additional data which may integrate the datasets in the project related to SIGINT signals are: georeferenced and dated location, emitters' technical parameters (usually parameters such as Frequency, signal accuracy level, pulses duration and repetition). Even in the event of receiving this information associated with a technical fingerprint, it is not possible to link these with the identity of any individual. Therefore, these data are non-personal data. Transmitted messages through radio signals are explicitly excluded from the datasets, since the former only constitute signal detection. The risk of eavesdropping in these signals is totally excluded in the scope of project THEIA.

This description of the processing of information within the project do not bind the further use of the THEIA platform by end-users. As described in section 5. Signal intelligence (SIGINT) and the roles of RF in Deliverable D7.1 – "Assessment of current and planned EO (Optical & SAR) micro and pico-satellites and RF satellites mission", final users of the technology may need to comply with other laws, at European level (e.g. Law Enforcement Directive[12]) or national level in the use of these technologies.

5.2.4 Crowdsourcing information and personal data

Crowdsourcing information is a technique to obtain and process massive amounts of data from the Internet. It is relevant in the scope of THEIA project for the development of capabilities to detect threats nearby border areas, and to prevent potential mass population movements that may derive in emergencies situations. As described in Deliverable D3.1 – "THEIA Ethics version 1 (1st period)", it is one element of research in THEIA for the strengthening of Copernicus Security Services and EU governmental crisis management capabilities in the area of forced population

[11] Guidelines 07/2020 on the concepts of controller and processor in the GDPR European Data Protection Board 2021.

[12] 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.

displacement. The use of open-source data to detect and anticipate potential movements of groups of population is a capability explored through the research in the project.

The implementation of these advanced techniques of information analysis seeks the improvement in accuracy and relevance of the use of aggregated personal information. Ethical principles must be considered and fully respected when collecting such data. The development of this technical tool in THEIA involves the integration of a multi-source extraction framework, drawing from a diverse pool of publicly available sources, including social media platforms. The main objective is to test and develop an algorithmic tool of analysis of aggregated information that could be at the disposal of the public administration law enforcement entities to better assess security risks, for their identification, analysis, and mitigation. Further details on the deployment of the tools are expected to be included in Deliverable D8.1 "Delivery of the crowdsourcing tool".

Websourcing is an information gathering technique already explored in scientific literature[13], with potential impact on privacy of individuals[14]. It must be developed under strict guarantees for the fundamental rights of individuals, and under exceptional and justified circumstances.

The development of the crowdsourcing tool in THEIA is built a stateless processing and forwarding component, handling only non-personal data. These principles ensure the use of only anonymised data. The sources of the data are selected social media applications and open-source websites with publicly available data. That information is extracted through an API that anonymises the information in extraction. The objective is to exclude any possibility of identifying the individuals. The workflow pushes the data into the THEIA platform environment in an anonymised format. These elements exclude the information from the definition of personal data in article 4 section 1 of the EU General Data Protection Regulation. The system is designed to operate without collecting information that could directly or indirectly identify an individual. Data which could potentially be present in the environments of extraction, such as names, email addresses, usernames, IP addresses linked to individuals, device identifiers, or authentication data are excluded, or anonymised in the source. The only channel of transmission of the data from the source is the secure APIs to the THEIA platform. The data is not stored locally or persistently within any other environment. Once transmission is completed, no residual data

[13] Daniel J Solove and Woodrow Hartzog, 'The Great Scrape: The Clash Between Scraping and Privacy' (2024) 1521 California Law Review 113.
[14] Taner Kuru, 'Lawfulness of the Mass Processing of Publicly Accessible Online Data to Train Large Language Models' [2024] International Data Privacy Law ipae013.

remains within the tool. The crowdsourcing tool cannot be used to re-identify individuals, either directly or through data correlation. There is no data persistence, logging, or historical storage of processed information. This design amount to data protection by design and by default measures defined in article 25 GDPR. The practice of the European Data Protection Board confirms this approach, as the measures are considered "*at the time of the determination of the means for processing*", i.e. during the design and testing of the crowdsourcing tool, and "*at the time of the processing itself*" (maintenance and review of data protection requirements are possible for the end-users in the application of the tool to real-deployment scenarios)[15].

The Court of Justice of the European Union considers the exercise of anonymising personal data as a data processing operation itself[16,17]. However, the anonymisation process occurs outside of the scope of the research in project THEIA, because of the automatic system through the APIs.

The development and use of the APIs for the access of aggregated data in social media apps normally relies on the legal basis for the development of the scientific research under article Article 89 GDPR. This is also the case for the THEIA project, in view of the developments of aggregated information for the access to the information on source and the anonymisation process[18].

Even if the processing of personal data is excluded through the crowdsourcing tool in THEIA, additional safeguards are developed to the processing, that may qualify as data protection by design and by default. As part of the security and privacy by design and by default principles (article 25 GDPR), strict authentication mechanisms and restricted access to data with role-based access control are established. The anonymisation in the source (through the API accesses in the social media platforms) assigning a hash to the usernames excludes the possibility of profiling under article 4 section 4 GDPR. The application of these measures lowers the risks of re-identification of the social media users and guarantees anonymity in the aggregation of information.

[15] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, European Data Protection Board 2020.
[16] *Single Resolution Board v European Data Protection Supervisor (EDPS v SRB)* [2023] Court of Justice of the EU Case T-557/20, ECLI:EU:T:2023:219.
[17] Breyer v Bundesrepublik Deutschland [2016] Court of Justice of the EU, Case *C-413/23 P,* ECLI:EU:C:2016:779.
[18] Svanberg, Christian Wiese, Article 89 Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in Christopher Kuner (ed.), and others, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020), p. 1240–1251.

The further use of this tool by end-users goes beyond the scope of the research project, and will need to comply with existing regulations governing personal data, the right to privacy, and respect for private life of individuals.

5.2.5 Data protection impact assessment

A Data Protection Impact Assessment (DPIA) is a comprehensive legal analysis in a structured, documented, ex ante format, containing a risk assessment carried out by a controller, where planned processing operations are likely to result in a high risk to the rights and freedoms of natural persons, aimed at evaluating necessity and proportionality, identifying risks, and determining measures to mitigate them in accordance with the accountability principle under Article 5 section 2 of the General Data Protection Regulation.

The development of a DPIA is mandatory only when the processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons. For the rest of processing operations, it constitutes an additional data protection by design and by default measure, which helps documenting of the rest of appropriate safeguards and technical measures developed to protect the personal data from foreseen lower-impact risks. Art. 35 paragraph 3 specifically lists the case where a data protection impact assessment shall be required:

a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
b) processing on a large scale of special categories of data referred to in Article 9 section 1, or of personal data relating to criminal convictions and offences referred to in Article 10; or
c) a systematic monitoring of a publicly accessible area on a large scale.

The minimum content of the assessment in established in GDPR is: a description of the processing and its purposes; an assessment of the necessity and proportionality of the processing in relation to these purposes; an assessment of the risks to the rights and freedoms of data subjects; the measures envisaged to address the risks, including security measures and mechanisms, to ensure the protection of personal data and to demonstrate compliance with the GDPR. This content is

detailed by the European Data Protection Board in its specific Guidelines on Data Protection Impact Assessment[19].

Research in project THEIA does not foresee any of these situations. Therefore, there is not any need established to develop a Data Protection Impact Assessment for the project research as a whole. Any risk associated to processing of personal data within THEIA project's lifetime is considered low. This evaluation does not preclude the possibility of specific processing or research activities being evaluated by any of the partners using their own individual DPIA. It neither should preclude the potential analysis, voluntary or mandatory, developed by the end-users in the deployment of the THEIA platform, or the use of the technical capabilities developed in the project.

5.2.6 Demographic data analysis

Part of the research in project THEIA under Task T8.2 consists of the curation and analysis of existing statistical, economic, demographic, and environmental data in order to establish a comprehensive baseline database for the Areas of Interest (AOIs). These data provide essential insights into socioeconomic conditions and demographic dynamics that are critical for identifying, contextualising, and understanding patterns of forced displacement. Information is obtained from governmental and international organisations, including the United Nations (UN), the United Nations High Commissioner for Refugees (UNHCR), and the International Organization for Migration (IOM), among others. The datasets cover population characteristics (such as age distribution, gender, and household composition), crime and conflict indicators, labour market and employment metrics, poverty and economic vulnerability measures, as well as education and literacy rates. In addition, environmental variables of natural and man-made disaster events are incorporated. The objective is to offer an integrated and multidimensional database relevant to forced population displacement and identify key socio-economic, demographic, and environmental indicators associated with displacement events.

The partners involved in the delivery of the Statistical, Economic and Other Demographic data state the complete exclusion of personal data of the datasets, due to the access only to publicly available information and data published by International Organizations with low granularity.

[19] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Article 29 Data Protection Working Party, 2017, (17/EN WP 248 rev01).

6. Ethics by design in THEIA

6.1 Ethics manager

In order to ensure due attention to all the ethics issues that may emerge in the project, the THEIA consortium has decided the appointment of an Ethics manager. The Ethics manager is an internal member of the consortium. The appointment is decided for Prof. Dr. Vagelis Papakonstantinou.

His role and responsibilities will be the following:

1. Address ethical issues and coordinate their response in collaboration with the Project Coordinator, the Security advisory board (SAB) and the Data Manager.
2. Communicate the actions developed in terms of Ethics to the rest of the partners in the consortium, particularly those developed within WP3 – Ethics 1 - 1st period and WP4 – Ethics 2 - 2nd period.
3. Identify and periodically reassess ethical risks across work packages.
4. Ensure that required ethics approvals (e.g., from research ethics committees, or competent authorities) are obtained prior to the start of relevant research activities.
5. Coordinate the communications of ethical relevant affairs with the Project Officer, the external reviewers, the European Commission, with due involvement of the consortium, particularly its Project Coordinator.
6. Manage the direct communications with the Ethics Advisor. Ensure their correct involvement and information. Defend the independence of the Ethics Advisor and communicate the problems that may emerge in the development of their work to the consortium. Provide the information necessary for the development of their consultation role. Assist in the drafting of informed ethics opinions within the project, for their external evaluation.
7. Coordinate the action and information of the Data Protection Officers of the partners within the project research scope (ParDPOs), or the responsible contacts to ensure compliance with data protection regulations.

The Ethics Manager attends to the relevant internal meetings in the project. The Consortium must guarantee that he has the chance to speak and voice its opinion on ethics matters, whenever necessary. They must grant limitless information and access to project documentation in order to ensure the development of his tasks.

The appointment of the Ethics Manager was developed in the first stances of the project. Its description of tasks follows the consideration of recommendations in the last external review engagement. The General Project Review Consolidated Report (He) issued on 02/10/2025

established a specific Expert opinion on deliverables in its Annex 1. Amongst those elements, the reviewers recommend: "*As an Ethical Manager is mentioned in D1.3 Initial Data Management Plan (DMP), a detailed description of its role and responsibilities should be included in the updated version of the OEI deliverable, i.e. D3.2 - THEIA Ethics version 2 (1st period) which is due in M15.*" This request is addressed in this section of the present report.

6.2 Internal protocol for ethical procedures. Incidental findings.

In the course of the development of the research in project THEIA, incidental findings that are potentially relevant in terms of ethics may arise. This incidental findings policy tailors the response to these discoveries. It lays down the policies that will address the procedures and the responsibilities for communicating to the respective authorities. Incidental findings are traditionally defined as "results that arise that are outside the original purpose for which the test or procedure was conducted". In the THEIA project, in the event of any incidental finding raising ethical concerns discovered throughout the execution of the project, the following actions will apply:

1. In a first place, these incidental finding will be immediately referred to:
    a. the project's responsible partner for the concrete research action,
    b. to the person with the closest link with the research participant,
    c. to the Project Coordinator,
    d. only if the finding has an ethical relevance, to the Ethics Manager, and
    e. only, if necessary, to the Ethics Advisor and
    f. the European Commission, in its Funding Agency capacity, via the Project Officer with the view to evaluate their ethical implications and to reach a decision on further action.
2. Secondly, the following rules will govern any incidental findings:
    a. individuals will give an informed consent to take part in the research;
    b. deletion of any incidental findings will be considered by the bodies mentioned in (1);
    c. in case of incidental findings that include recording an illegal activity, the consortium will comply with all relevant national and international laws;
    d. in case of incidental findings that include any information of public interest, the bodies mentioned in (1) would make a decision about the need, means and timing of their communication to relevant stakeholders.

The incidental finding policies of THEIA should conform to these basic requirements, including those established individually by the project coordinator. These requirements may be revised and adjusted throughout the lifetime of the THEIA project. The incidental findings policy reflects on the ethical complications stemming from new forms of risk, threats and vulnerabilities and the multiple meanings and normative implications of emerging technologies.

7. THEIA Ethics advisor

7.1 Role of the advisor

As per Task 3.1 of project THEIA, developed in its Description of Action, a report on D3.1 "THEIA Ethics version 1 (1st period)" was issued on month M3 of the project (February 2025). The General Project Review Consolidated Report (He) issued on 02/10/2025 established a specific Expert opinion on deliverables in its Annex 1. Amongst those elements, the reviewers recommend: "*Moreover, to ensure full compliance with ethical standards, at least one independent ethics advisor (separate from the SAB) should be appointed.*" A list of candidates was elaborated to appoint an Ethics Advisor for the project. The candidate chosen is presented with the Terms of reference and a Non-Disclosure Agreement (NDA), to compromise for this role.

In this report, we offer the Terms of reference for this role. This document describes the actions and interactions that the Ethics Advisor will develop in the project. It also ensures the necessary commitments of the consortium to align to the Ethics Advisor's action, and offer the information and resources necessary to complete the abovementioned tasks. The Ethics advisor works in conjunction with the Security Advisory Board and the Ethics Manager of the project, the Data Manager, the Data Protection Officers of the partners, the Project Coordinator, and the rest of researchers and stakeholders involved in project THEIA. An overview of these positions and responsibilities is offered in Deliverable D1.5 "Intermediate Data Management Plan (DMP)", section 2.4.3.

7.2 Ethics and confidentiality

This role of Ethics Advisor is therefore established, and will be maintained during the whole duration of the project. Its aim is to externally monitor the progress of the project, identify possible ethical and legal issues, and suggest solutions to be put in place by project partners. After signing a NDA, which is necessary to gain access to the confidential information produced by THEIA, the key deliverables and reports are provided to seek the opinions and advice of the Ethics Advisor.

The Ethics Advisor acquires a commitment to undertake its external counseling role with due respect to confidentiality. By the signature of the NDA, it enters into a legally binding compromise to develop this activity with due respect and consideration of communications secrecy. The Ethics Advisor must develop its tasks under the instructions of the consortium partners when processing of personal data, or confidential information.

Nevertheless, these compromises should not hinder its independence to assess ethical aspects in the project with due objectivity. Special attention should be considered to communications

labelled as sensitive, via email, or any other form of engagement in the consortium, and to deliverables and reports with a "Confidential" or "Sensitive" status.

These obligations must be interpreted and developed with due attention to the principles of Open Science. THEIA project engages in scientific research developed in an open cooperative methodology, and systematic sharing of knowledge and tools as early and widely as possible in the process, as established in the European Commission Horizon Europe Programme Guide[20].

7.3 Overview of tasks

The following Terms of reference are elaborated for project THEIA considering the guidelines of the European Union institutions on Ethics Advisors and Ethics Advisory Boards: Roles and Function in EU-funded Projects[21].

The Horizon Europe program emphasises the importance of ethics in all forms of research[22]. The THEIA consortium must adopt a set of procedures, outlined in Work Package number 3, Tasks T3.1 and T3.2, and Work package number 4, Tasks T4.1 and T4.2 of the THEIA project. These procedures are dedicated to ensure that both its activities throughout the project, and the final output of the research, respect and comply with recognised standards of research ethics.

The Ethics Advisor is the advisory entity tasked to follow and closely monitor the project activities that could raise ethical issues. The European Commission perceives 'ethics' as including questions of legal and regulatory compliance as well as a branch of philosophy. It is part of a process of 'governance'. In this vein, the EC specifies that the role of Ethics Advisors should be seen as "the EC fulfilling its obligations to help avoid public uneasiness towards science and to mitigate concerns where they exist."[23].

A key prerequisite of the role of Ethics Advisor is independence, seen as objectivity and impartiality. For this reason, the Ethics Advisor should be free of any conflict of interest, and their activity is formally independent of the project's work packages.

[20] Horizon Europe Programme Guide, version 5.1 (2025) https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/programme-guide_horizon_en.pdf

[21] Ethics Advisors and Ethics Advisory Boards: Roles and Function in EU-funded Projects. European Research Council. Version 2.0. 15 February 2023. Available at https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/roles-and-functions-of-ethics-advisory-ethics-advisory-boards-in-ec-funded-projects_he_en.pdf .

[22] Cf. Rome Declaration on Responsible Research and Innovation in Europe, 21 November 2014, https://ec.europa.eu/research/swafs/pdf/rome_declaration_RRI_final_21_November.pdf

[23] Ethics Advisors and Ethics Advisory Boards: Roles and Function in EU-funded Projects. European Research Council. N.1.

The tasks of the Ethics Advisor include the independent review of research results in the project. It also includes the elaboration of informed opinion whenever required, and particularly, in case of direct consultation by the consortium. These consultations are addressed by the Ethics Manager, with involvement of the Project Coordinator, and informing duly the consortium partners.

7.4 Roadmap for future involvements and recommendations

The following roadmap is tentatively designed for the engagement of the Ethics Advisor in the research in project THEIA:

1. M15 – Appointment of the Ethics Advisor. Signature of the Terms of Reference and NDA. Official onboarding in the project as an external advisor. Invitation to attend (in person or virtually) to the Project Plenary Meeting. Presentation by the Ethics Manager of the role, responsibility and person.
2. M16 – The Ethics Advisor receives the main deliverables and reports already elaborated in the project, for consultation.
3. M18 – The Ethics Advisor elaborates the first Independent assessment report.
4. M24 – The Ethics Advisor receives the main deliverables and reports already elaborated in the project, for consultation.
5. M26 - The Ethics Advisor elaborates the second Independent assessment report.
6. M30 – The Independent assessment reports are included in the content of deliverable D4.1 – THEIA Ethics (2nd period). An indication of the actions taken by the consortium to comply with the indications of the Ethics Manager is also offered in the report.
7. Date to be confirmed – The Ethics Advisor is invited to attend to the following General Assembly meetings and Plenary meetings, as well as the rest of engagements with the European Commission as financing entity of the project.

The NDA signed by the Ethics Advisor is stored in the project repository. Annex I of this report contains the Terms of reference template which are signed by the Ethics Advisor.

ANNEX I

Terms of reference Ethics advisor

Terms of reference

for External Experts

in their role as Ethics Advisors to the project

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

THEIA

Grant Agreement No 101190051

NAME OF EXTERNAL EXPERT: _____

Located at _____.

hereinafter referred to as "**Ethics Advisor**"

and

GEOSYSTEMS HELLAS IT KAI EFARMOGESGEOPLIROFORIAKON SYSTIMATON ANONIMIETAIREIA - Geosystems Hellas S.A.

located at _____

hereinafter referred to as "**Coordinator**",

signing and acting for and on behalf of itself and all other partners of the THEIA Consortium, a Project funded under the Horizon Europe Programme (HORIZON-CL4-2024-SPACE-01), Grant Agreement number 101190051 (hereinafter referred to as "**Project**").

1. Preamble

1.1 This document summarises and communicates the main tasks for the Ethics Advisor for Project THEIA. This document is addressed to different stakeholders:

1.1.1 The Ethics Advisor, who is considered an external member of the project. This document collects their functions and role. These areas of assistance in the Project are described here.

1.1.2 The partners of the THEIA consortium. As per the signature of this document, they acknowledge the identity of the Ethics Advisor, the role and engagement expected from the external expert, and their obligations to provide the information and resources necessary to complete the tasks of the Ethics Advisor.

1.1.3 Other stakeholders and external supervisors. As part of the compromise and fulfilment of the societal and ethical obligations of the consortium, this document will be accessed by the evaluators of the Project.

1.2 As per this document, and the development of their roles and responsibilities, it is considered that the Ethics Advisor is an individual ethics expert who provides advice on issues of ethical relevance which relate to the planned and/or ongoing research in the context of project THEIA, an EU-funded project, and, if required, reports to the Commission/Executive Agency/Funding Body.

1.3 The Ethics Advisor ensures impartial and independent oversight of the research in the Project. He or she will be report after each phase of the project research, ensuring that the results of the research are evaluated, and respective recommendations are implemented by all partners. Compliance with the relevant laws and norms is achieved through the implementation of these recommendations.

2. Contact points of information

2.1 The Ethics advisor must work in conjunction with the Security Advisory Board and the Ethics manager of the project, the Data Protection Officers of the partners, the Project Coordinator, and the rest of researchers and stakeholders involved in project THEIA.

2.2 The Ethics Coordinator of the project must keep the Ethics Advisor informed on the latest activities and developments of the project. The Ethics Coordinator will periodically report to the Ethics Advisor concerning ethical issues or aspects that arise throughout the project life, including the issues that the Consortium has discussed or faced internally and are not reflected in its deliverables.

3. Initial engagement of the Ethics Advisor

3.1 In order to receive not only public, but also confidential information, the Ethics Advisor is expected to sign a non-disclosure agreement. With access to a wider range of documents, produced by THEIA, the engagement, and thus the assistance, of the Ethics advisor can be more in-depth and useful for the INTREPID consortium.

3.2 The consortium will offer an overview of the information and outputs of the research develops prior to the incorporation of the Ethics Advisor to the project.

3.3 These Terms of reference describe the general tasks and activities in which the experts will engage as Ethics Advisor to the Project. The tasks described here must be interpreted in light of the Grant Agreement and Description of Action subscribed between the partners of the THEIA project and the European Commission Research Executive Agency, and in light of the Consortium Agreement signed by these partners.

3.4 Upon acceptance, the Ethics Advisor will be requested to sign the Non-Disclosure Agreement. The signature of this legally binding document is marked as the start of the external collaboration of the Ethics Advisor in project THEIA. The sharing of documents and confidential information will only occur after this signature.

4. Description of Tasks and ethical advice

4.1 The Ethics Advisor develops tasks of ethical advice to the project. The Ethics Advisor must:

4.1.1 Impartially assess and validate the measures adopted by the consortium to comply with ethical and legal standards.

4.1.2 Provide external expertise, flag areas of ethical or legal concern.

4.2 The responsibilities of the Ethics Advisor are:

4.2.1 To provide independent advice and feedback about ethical issues arising in the project, by monitoring specific activities or selected deliverables deemed to be 'ethically sensitive'.

4.2.2 To alert the consortium about any ethical issues that are seen as actual or potential. It is the duty of the project coordinator to reply to the alerts and to collaborate closely to address those issues effectively.

4.3 These actions will be completed by the analysis and emission of informed opinion documents. The Ethics Advisor will be presented with a number of documents with ethical and legal relevance to the project. Prior to the meetings scheduled every year, the Ethics Advisor will study them and must be ready to provide an opinion from the legal and ethical point of view.

4.4 The external Ethics Advisor must be free of any conflict of interest, and their activity formally independent of the project's work packages'.

4.5 A specific amount per year is reserved in the project budget to cover necessary travel and subsistence expenses of external experts for attending and delivering presentations on the topic at the project plenary meetings, general assembly meetings and workshops. There is not any other remuneration for the Ethics Advisor foreseen for the participation in the THEIA project. The Ethics Advisor role is an unpaid position.

5. Specific engagements and meetings

5.1 The Ethics Advisor has the right to attend to the project plenary meetings, general assembly meetings and workshops, under the compromise of confidentiality to the matters discussed in these meetings, and without any voting rights. The attendance is not mandatory, insofar

as the tasks described in these Terms of reference may be completed without it. The attendance to these meetings may be in physical presence, or online.

6. Confidentiality

6.1 Before the joining of the Ethics Advisor to the external engagement in project THEIA, it is presented with a Confidentiality Undertaking to sign and serve as a Non-Disclosure Agreement. This unilateral compromise covers the reception and use of the confidential information during the activity of THEIA project, and after the project has finished. To this respect, the THEIA consortium declares:

6.1.1 The THEIA Partners desire to collaborate with the Ethics Advisor with respect to the performance of the abovementioned advisory activities;

6.1.2 In order to perform said activities, the Ethics Advisor needs to access technical and/or commercial information of a confidential or proprietary nature presently in the possession of the THEIA Partners, which wish to ensure that the same remains confidential.

6.1.3 This information is communicated to the Ethics Advisor for the purposes defined in these Terms of Reference. The Ethics Advisor undertakes not to use the Confidential Information for any reason except these purposes, and not to process any personal data received with it for any different purpose as the indicated by the controllers.

7. Incidental findings

The Ethics Advisor acquires the compromise to communicate any potential incidental findings in the THEIA research to the Project Coordinator and the Ethics Manager in the first place. As well as any ethically relevant elements or disruptions in the research in project THEIA. They will assess the situation, inform duly to the partners of the consortium, and coordinate the reporting obligations to the European Commission.

Name of "External Expert" Authorised signatory: *[NAME]*

Date: *[DATE]*

Signed

Receiving Party

Name of authorised Member of GEOSYSTEMS HELLAS IT KAI EFARMOGESGEOPLIROFORIAKON SYSTIMATON ANONIMIETAIREIA Geosystems Hellas S.A - **GSH** acting on behalf of the consortium:

Name

Position

Signed

ANNEX II

Partners' responses to the Ethics Questionnaire

Q1.1. Which type of organisation do you represent in the Project?

- ○ End user
- ◉ Project partner
- ○ Stakeholder

Q1.2. Type-in the name of your organisation or the partner you represent in THEIA project

GEOSYSTEMS HELLAS

Q1.3.
Please, type-in your name.

Your name will not be shared with anyone, neither with the other partners of the Consortium, nor published with the survey. It will only be used if internal checking of the results, or feedback is needed by MPLegal.

Q2.1.
Which technology or process is developed or used by your organisation in the project?

- ☑ Data processing pathway
- ☑ Users requirements coordination, demo activities and use-cases
- ☑ Very-High-Resolution Earth Observation tools (Thermal imaging and low-visibility sensing)
- ☑ Very-High-Resolution Earth Observation tools (Data acquisition: Space-based video)
- ☑ Very-High-Resolution Earth Observation tools (Data acquisition: Satellite-Based Multi-Payload Data)
- ☑ Data acquisition: Micro-satellites & Cubesats
- ☐ Data acquisition: UAS-based data
- ☐ Integration of the multi-sensor platform
- ☐ Testing sensors on drones. Drones deployment for testing in real conditions
- ☑ AI for detecting and tracking objects
- ☐ THEIA crowdsourcing tool
- ☑ Database for the Areas of Interest
- ☐ High-velocity transnational data
- ☐ Data fusion & Data models. Data exchange framework

- [ ] Data exchange platform for cloud infrastructure to satellite data
- [x] National Constellation Data Federation
- [ ] Optimized API Access
- [ ] GeoAI. UAS and terrestrial sensor-based image processing
- [x] GeoAI. Georeferencing
- [ ] GeoAI. Intelligence Gathering
- [ ] GeoAI. Fusion and GeoAI Module
- [x] THEIA platform
- [x] Demonstration and validation activities
- [x] Communication, Dissemination, Training and Exploitation
- [x] Others

Q2.2. If Others, please specify which ones, and within which Work Package in the project.

Overall architecture (WP5)

Q2.3. Briefly describe the objectives and possible benefits of the development and use of the technology in the project.

Data-processing pathway Objectives Achieve low-latency and relative-to-the-use-case data retrieval Possible benefits The end-user receives the results he/she needs, in a timely manner. Results, in the sense of the output of the computation performed on the data retrieved by the platform. User requirements coordination, demo activities, and use-cases Objectives Form a set of URs which adress the gaps of the CSS Form a set of use cases which will guide the demo activities. Possible benefits Extend the CSS in a useful way VHR EO tools (images) Objectives To detect tents, vehicles, vessels of specific properties (geometric, etc) Possible benefits Enable the end-users to cooperatively decide on how to deal with a developing emergency. VHR EO tools (video) Objectives Provide to the end-user, tracking information, ie detected objects which are moving Possible benefits The end-user gets fuller situational awareness, through observing the kinetic behaviour of the objects of interest. The end-user can make better decisions in order to prevent damage to the EU or the people which are using the detected objects. Data acquisition: Microsats and Cubesats Objectives Same as with the case of VHR satellite data Possible benefits Achieve more dense coverage, in both space and time, of the AOIs AI for detecting and tracking objects Objectives Enable the end-users to make decisions based on both static and moving material, concerning the objects of interest Database for the areas of interest Objectives Archive the detections and the trackings provided by the relevant tools of THEIA. Possible benefits Enhance the decision-making capabilities of the end-users by providing not only current, but older data. National Constellation Data Federation Objectives To provide fuller, in a both spatial and temporal sense, coverage of the AOIs. Georeferencing Objectives To provide the location of the data output by the algorithms of the platform. Possible benefits To enable the end-users to act upon the observations. If the observations are not placed in space, with a sufficient location accuracy, crucial time can be lost. If no georeferencing is provided, observations are cannot be acted upon. THEIA platform Objectives To provide to the end-users collaborative capabilities, utilising a variety of actionable data, fused and non-fused. The context is operational. Possible benefits Realisation of all the URs. Demonstration and validation activities Objectives Design and conduct use cases and demo activities Assess the THEIA solution. Possible benefits Gather material utilised for the improvement of the THEIA solution. Communication, Dissemination, Training and Exploitation Objectives Maximise the impact of the project Overall architecture Objectives To provide a schema which (a) clarifies the components/modules (b) the technologies Possible benefits To establish a common technical view of the THEIA solution

Q3.1.
Are you processing or intend to process personal data when developing or using these technologies in THEIA?

Please keep in mind that the terms 'personal data' and 'processing' are rather broad. Processing means the use of personal data at any stage of the Project: collecting, recording, studying and publishing these data, amongst others. Personal data are any information relating to an identified or identifiable natural person. For instance, in THEIA: the processing of a dataset including footage with a camera that records people, the curation of intelligence data from publicly available sources or social media about individuals behaviour, or the collection of information from potential end-users that identify the counterparts, or interaction with them. All these activities imply the processing of personal data, and require an affirmative answer. On the other hand, processing datasets that solely include technical data about UAVs, satellites signal, or geo-spacial

resources would not be considered processing of personal data. ***When in doubt, you generally process some personal data. If you have any questions about this, or do not exactly know if you process personal data, please contact MPlegal before continuing with the survey.***

- (●) Yes
- ( ) No

Q3.2.
Please specify the types of personal data which you process.

The categories below are provided for orientation and are not necessarily needed for the purposes of the project. Please specify those relevant to your activities.

- [x] a) Identification data (e.g. name, data of birth, age, gender, address, email, phone number)
- [x] b) Personal features
- [ ] c) Financial data
- [x] d) Physical, physiological or behavioural characteristics, of a natural person, allowing his/her identification.
- [ ] e) Genetic data
- [ ] f) Biometric data
- [ ] g) Other information regarding health, incl. mental health
- [ ] h) Habits
- [ ] i) Family composition
- [ ] j) Hobbies and interests
- [ ] k) Consumption patterns
- [ ] l) Residence or home address
- [ ] m) Education
- [ ] n) Occupation, employment or professional affiliation
- [ ] o) Social security number or other national identification codes (Passport or ID number)
- [x] p) Racial or ethnic background
- [ ] q) Philosophical or spiritual orientation
- [ ] r) Information on sexual preferences
- [ ] s) Political orientation or opinion
- [ ] t) Membership of trade union or affiliation
- [ ] u) Other memberships
- [x] v) Video footage of individuals
- [ ] w) Others

Q3.3. Develop your previous answer, if it is necessary for any category, or if you clicked "Others".

Q3.4.
How will you obtain the personal data?

- [ ] Directly from data subjects
- [x] Other partners
- [ ] Other sources
- [ ] I do not know

Q3.5. Please specify the sources and means of receiving with regards to all the categories of personal data.

- [x] Sensors
- [x] Video recordings
- [ ] Software
- [ ] Website
- [ ] Questionnaires
- [ ] Existing datasets
- [ ] Other means
- [ ] I do not know

Q3.6. Develop and classify per set of personal data the sources.

E.g. Identification data (name and email) are obtained directly from data subjects through a website. Biometric data (facial geometry) are obtained from existing datasets through

Sensors and video recordings The consortium possibly contains sensors of sufficient accuracy, in order for a person to recognised. This applies to both image and video data.

Q3.7. People need to be informed of the processing of their personal data, unless they are obtained indirecty or anonymised. How do you inform the data subject about the processing activity of personal data?

Please come back to MPlegal with any questions regarding this aspect.

If any personal data are captured by the peripheral components, or produced by them, then they must inform the subjects about this.

Q3.8.
Whose personal data is being processed?

Please describe the data subjects, i.e., the individuals or groups of research participants whose personal data will be collected and processed during the project.

You are kindly redirected to the peripheral components which will process personal data, if any exist.

Q3.9.
How will you arrange the personal data?

Please describe the datasets of personal data that you have, and map basically your information flows (i.e. what data, where it comes from and where it goes – if it is within your organisation, mention the department; if outside, which partners. **This needs to be a basic answer, which will be developed and used as a base for developing a Data flow map in next deliverables for THEIA.**

You are kindly redirected to the peripheral components which will process personal data, if any exist.

Q3.10.
What do you want to achieve by collecting the personal data?

Please describe for all the categories of personal data.

Concerning the central database of THEIA, personal data are of know use.

Q3.11.
How will you use the personal data?

Please describe briefly and precisely for all the categories of personal data.

Concerning the central database of THEIA, personal data are of know use.

Q3.12.
Is the processing of the personal data really necessary to achieve your purpose?

- ○ Essential
- ○ Important
- ○ Accessory
- ◉ Not necessary

Q3.13. Have you explored alternative means to the use of personal data? (mock data, anonymous dataset, fewer variables of personal data…) How satisfactory would they be to achieve the same outcome?

- ◉ No, I have not explored them.
- ○ Yes, I know them. They would not be effective for the purpose.

- ◯ Yes, I know them. They are currently under use.
- ◯ No, we have not explored them. We will incorporate them in the future.

Q3.14.
Where will the personal data be stored?

Please explain the location

- ☑ Locally, in corporate servers, including those accessible remotely via cloud.
- ☑ Locally, in corporate devices.
- ☑ Cloud
- ☐ Third parties servers
- ☐ Other

Q3.15. Where are these servers / storage of personal data?

- ◉ In a country member of the European Union
- ◯ In a country outside the European Union
- ◯ Unknown

Q3.16.
Will you share the datasets of personal data with third parties, not members of the THEIA consortium?

- ◯ Yes
- ◉ No

Q3.17.
If yes, please explain the reasons and name the receivers. Please specify if these receivers are located in the European Union or abroad.

-

Q3.18.
Will you cooperate with other partners or external entities for the processing of the personal data?

- ◉ Yes
- ◯ No

Q3.19.
***If yes**, please specify:*

- ○ We need the cooperation as assisting in our processing activities, and for our own purposes.
- ◉ We negotiate and control together the collaboration. We define jointly the purposes of the processing.
- ○ Other engagement.

Q3.20.
If you engage with other entities to assist you in data processing, what type of work do they develop? How do you make sure that they comply with data protection principles?
Please describe data types and purposes of joint processing.

Joint processing in GSH's case, takes the meaning of receiving personal data, if any, by other partners, and store them. Also, receiving streaming data from partners, and displaying them. If personal data are necessary to be received from other partners, and stored to the database, one measure is to enforce a field specifying if personal data are to be stored. That field must be filled in automatically, by the peripheral component which sends the personal data. Similar fields which convey information useful for securing data protection principles must be defined by the peripheral components. Those fields can be used by the storage component, so that possible rejection of the data happens, or, if accepted, the data will be treated according to the data protection principles. Eg deletion after a specific time window. It is stated that currently, three different points are identified as data-protection points. The first one is the peripheral. The second one is the central, before data are stored to database. The third one is the UI.

Q3.21.
Will you work with an external online tool, or other cloud computing solution to process personal data?
If so, which one? Do you know the geographical location for storage of information of such tool or cloud servers (e.g. Europe, US, Canada, Japan)?

The central database of THEIA will be running on a CREOTECH VM.

Q3.22.
In your view, do you think you will need to store the personal data collected for this project after its ending?

Could you please provide a justification, in the light of the purpose for which you process personal data?

No, no storage of personal data is necessary.

Q3.23.
Would you be willing to anonymise the data?

Data anonymisation *is a process applied to personal data after which it is no longer possible, now, or in the future, to trace the identity of the individual. It is normally done by separating the elements in the dataset that allow identification. Or assigning random codes of identification to the datasets that cannot be traced back to the original data subject, through encryption.*

- ◉ Yes
- ○ No

Q3.24.
***If no**, please provide the reasons.*

Q3.25.
Would you be willing to pseudonymise the data?

Pseudonymisation *is a process applied to personal data, replacing the identifiable parts of the dataset with a code or reference number, using an agreed upon code. If you need it, you can reverse the process, and obtain back the individual identity through the used code.*

- (●) Yes
- ( ) No

Q3.26.
***If no**, please provide the reasons.*

Q3.27. Will you implement data protection by design and by default measures?

Some examples of these measures are providing the control to the data subject over his/her personal data once the technology is implemented. Or reduce the data needed and pseudonymise it.

- (●) Yes
- ( ) No

Q3.28.
If yes, develop which ones**. If not**, please provide the reasons.

By Design Authentication/authorisation Restrict access to a specific set of users. The uses which have access will have limited access, to the bare minimum of the data necessary. This will be achieved through the definition of roles and corresponding permissions, as prescribed in the architecture deliverable. Security of data in transit MQTT messages will be secured through SSL/TLS. HTTP messages will also be secured through SSL/TLS (HTTPS) Data at rest The exact measures against central database breach remain to be determined. The PostgreSQL database provides options such as password encryption, encryption of specific columns, and other encryption options.

Q3.29.
Will your technology be used for profiling data subjects and/or take automated decisions based solely on the processing of personal data from the data subject? This includes, amongst others, feeding Artificial Intelligence models with the data, in order to obtain decisions over these data subjects.

- ○ Yes
- ◉ No

Q3.30. If so, what kind of decisions?

Q3.31.
Do you follow or comply with any code of conduct or certification scheme in connection to the processing of personal data? For instance, ISO/IEC 27001:2022 standard for Information security, cybersecurity and privacy protection, Information security management systems; ISO/IEC 42005 Information technology — Artificial intelligence (AI) — AI system impact assessment, or the International Association of Privacy Professionals (IAPP) certifications.

- ○ Yes
- ◉ No

Q3.32.
Please identify and provide, if possible, the document or link to the document of certification.

Q3.33.
What will be the measures that you will take to secure the personal data that you process?

By Design Authentication/authorisation Restrict access to a specific set of users. The uses which have access will have limited access, to the bare minimum of the data necessary. This will be achieved through the definition of roles and corresponding permissions, as prescribed in the architecture deliverable. Security of data in transit MQTT messages will be secured through SSL/TLS. HTTP messages will also be secured through SSL/TLS (HTTPS) Data at rest The exact measures against central database breach remain to be determined. The PostgreSQL database provides options such as password encryption, encryption of specific columns, and other encryption options.

Q3.34.
Data subjects have certain rights under European law regarding the use and processing of their personal data. Do you already have a structure to ensure that data subjects are able to exercise their data subjects rights?

Some examples of these are the right of access to their personal data collected for the purposes of the project, right to erasure such data, right to rectification, right to data portability, possibility for the data subject to withdraw consent. The canalisations of those requests through a Data Protection Officer could be an example of an existing structure.

- ◉ Yes
- ○ No

Q3.35.
Please specify technical (e.g. specific email address for requests, software or in-built secure system allowing data subjects to access their own personal data in a transparent way) and organisational measures (e.g. who will provide the information to the data subject) to secure the personal data that you already put in place?

Will you need to limit those data subject rights? If so, please specify which one(s) and the reason to do so.

No personal data have been stored by GSH so far. Highly probable that there won't be any in the future.

Q3.36. How large is the volume of personal data that you process in the project?

- ○ Small
- ○ Large
- ◉ Not processing any personal data

Q3.37. Do you process any personal data of children?

Meaning underage people, below the age of 16 years old.

- ◉ Definitely not
- ○ Probably not
- ○ Probably yes
- ○ Definitely yes

Q3.38. Where do you obtain the personal data from children?

i.e. directly from them, from existing datasets, from their parents.

-

Q3.39. If you process personal data from minors, do you contact their parents/legal guardians? What information do you share with them about the data processing?

-

Q3.40. Are third parties involved in the processing of personal data?

- ◉ No.

- ◯ Yes, as contractors, performing some specific tasks under our instructions.
- ◯ Yes, we grant them access to the personal data.
- ◯ Yes, they have the same control over the data that we have.
- ◯ Yes, but we do not know the details.

Q3.41. Who are these third parties? What do they do with the personal data?

-

Q3.42. Please, justify your answer. For instance: we do not process personal data, because all the information that we use in the research project is technical data. Another cause will be that you access personal information, but you cannot identify individuals (anonymisation of personal data). Provide as many details as possible, and examples of the information.

This question was not displayed to the respondent.

Q4.1. Do you use existing datasets in your research in the project?

- ◉ Yes
- ◯ No

Q4.2. What is the origin of the datasets?

- ◯ They were in our possesion before the start of the project.
- ◉ They are publicly available.
- ◯ We obtained them after the start of the project free of cost.
- ◯ We obtained them after the start of the project with a licensing access commercial agreement.
- ◯ I do not know.

Q4.3. Do you consider that the datasets may include personal data in them? Please refer to the information in the previous questions from section 2 about personal data.

- ◯ Definitely yes. It is possible to identify individuals within the dataset.
- ◯ Definitely yes. The data are anonymised. There is personal information in the dataset, but it is not possible to identify the individual.
- ◯ Probably yes.
- ◯ Probably no.
- ◉ Definitely no.

Q5.1.
Do you think the use or development of the technology might impact privacy of individuals? (such as migrants, including displaced population due to armed conflicts or climate change, minors, undocumented people, and refugees)

Please keep in mind that privacy might be affected without processing of personal data (for example, drones flying above a private house, satellites capturing metrics of properties and terrain). **If you have any questions about this, or do not exactly know if privacy may be impacted, please contact MPlegal before continuing with the survey.**

- (●) Yes
- ( ) No
- ( ) Maybe

Q5.2. How does your use or development of the technology potentially impact privacy of individuals?

If a drone or a terrestrial sensor records by accident an individual

Q5.3.
Is this impact on privacy adequate and necessary to achieve the purpose for the development of this technology? For instance, develop the mission and mandate of a public entity, or provide a technical-tool/research that cannot be developed in any other way.

- ( ) Yes
- (●) No

Q5.4. Please explain why.

THEIA does not need information concerning individuals. The greatest level of approximation is a group of individuals. That is, the closest justified information, concerning human identity is the scale of a very big group of individuals. Specific info must be disregarded by design.

Q5.5.
Are there less invasive solutions that can be used to achieve the same purpose effectively?

- (●) Yes
- ( ) No

Q5.6. If yes, which are they, and why are they not used?

-

Q5.7. Do you think the benefits which result from the 'adequate and necessary' (research) activity are higher than the impact that it will cause for the privacy of the user?

- ○ Definitely Higher
- ○ Proportionate
- ○ Non-proportionate
- ◉ Lower

Q5.8. Please explain why.

The reason that personal data are of very limited importance for THEIA. It is

Q5.9. Does the implementation or use of the technology affect the subjects moral, religious or cultural integrity?

- ○ Yes
- ◉ No

Q6.1.
What would be, in your opinion, the benefit for the end-users of the technology and society?

Save migrants. Many times they are in danger due to traveling through the sea. Many times they are in danger due to exposure to attacks in the context of a conflict. They can be in danger due to adverse climate. Increase security of the EU. Highly-numbered human flows may include dangerous elements or directed efforts to violate the EU.

Q6.2.
Are there possible safety risks for the subjects related to the use of the technology?

- ○ Yes
- ○ No
- ◉ There might be.

Q6.3. Please, describe them, or justify the negative answer. For instance: there are risks, but we foresee safeguards that reduce them.

There are risks. These are not caused by the use of the technology though. However, a false positive might lead to deployment of Security Units without a reason, and expose them to danger without a reason.

Q6.4.

What technical and organizational measures can be taken to ensure and increase safety of the technology for end-users and data subjects?

Minimise False Positives, and maximise True Positives.

Q6.5. Are there any technical and organizational measures which could be taken to increase trust of the society and individuals in the use of the technology?

Adequate demo activities. Adequate dissemintaion activities

Q6.6.
Do you foresee any ethical issues related to the development or use of the technology?

- ○ Yes
- ◉ No

Q6.7. Please describe them.

-

Q7.1. Are the data used in the project susceptible of misuse? Could they be used, once processed, in a harmful way for the Project or for society?

No. The foreseen end-users maintain high ethical standards in their operations.

Q7.2. Are there any measures already implemented which would prevent this misuse to happen?

- ○ Yes
- ◉ No

Q7.3. Detail them or suggest new ones that could be implemented.

-

Q8.1.

Are there any risks of stigmatisation or discrimination, to your knowledge, in the use of these technologies in GeoAI and law enforcement?

The use of data for law enforcement is a sensitive domain for the general public. Particularly, border surveillance and security raises many societal and ethical questions. The treatment at large scale of information about borders and personal data about migrants needs to be performed in a comprehensive, sensible and protected way. Security measures and responses must be tailored to consider the needs and of vulnerable groups. The potential risk of misinformation must also be considered, as well as the potential generation or amplification of harmful stereotypes concerning these vulnerable groups.

- (●) Yes
- ( ) No

Q8.2. Are there any direct risks of misinformation associated to the use of these technologies?

- (●) Yes
- ( ) No

Q8.3. If any of these risks is spotted, what is the procedure you would follow to minimise and correct the affected stigmatisation or discrimination?

These risks could, technologically arise from modules with sufficient detection accuracy. However, it is sure that these modules will not record such data, and if they do, they will delete or anonymise them.

Q9.1. THEIA project has endeavoured to develop the research with attention to gender, inclusion, and adequate social norms. This requires not to consider, and not to inflict any negative gender stereotypes. The creation or propagation of gender stereotypes could lead to issues of discrimination for particular genders, or worsen other problematic already existing, and potential discrimination. Could the use of the technology help in tackling these stereotypes?

- ( ) Yes
- (●) No

Q9.2. How does it do so?

-

Q9.3. Are there any risks of amplification of gender issues in the use of your technology, or development of your research in the project? Please describe them.

There are not. Concerning Satellites, face recognition or other bodily properties is impossible with the foreseen satellite missions, and consequently the gender.

Q10.1.
If you consider that an important point has not been asked or you would like to make a comment for feedback, please type it down here.

THANK YOU FOR ANSWERING THE QUESTIONS!

Thanks for the comprehensive questionnaire.

Q1.1. Which type of organisation do you represent in the Project?

- ○ End user
- ◉ Project partner
- ○ Stakeholder

Q1.2. Type-in the name of your organisation or the partner you represent in THEIA project

European Union Satellite Centre - SATCEN

Q1.3.
Please, type-in your name.

Your name will not be shared with anyone, neither with the other partners of the Consortium, nor published with the survey. It will only be used if internal checking of the results, or feedback is needed by MPLegal.

Q2.1.
Which technology or process is developed or used by your organisation in the project?

- ☐ Data processing pathway
- ☑ Users requirements coordination, demo activities and use-cases
- ☐ Very-High-Resolution Earth Observation tools (Thermal imaging and low-visibility sensing)
- ☐ Very-High-Resolution Earth Observation tools (Data acquisition: Space-based video)
- ☐ Very-High-Resolution Earth Observation tools (Data acquisition: Satellite-Based Multi-Payload Data)
- ☐ Data acquisition: Micro-satellites & Cubesats
- ☐ Data acquisition: UAS-based data
- ☐ Integration of the multi-sensor platform
- ☐ Testing sensors on drones. Drones deployment for testing in real conditions
- ☐ AI for detecting and tracking objects
- ☐ THEIA crowdsourcing tool
- ☑ Database for the Areas of Interest
- ☐ High-velocity transnational data
- ☐ Data fusion & Data models. Data exchange framework

- [ ] Data exchange platform for cloud infrastructure to satellite data
- [ ] National Constellation Data Federation
- [ ] Optimized API Access
- [ ] GeoAI. UAS and terrestrial sensor-based image processing
- [ ] GeoAI. Georeferencing
- [ ] GeoAI. Intelligence Gathering
- [ ] GeoAI. Fusion and GeoAI Module
- [ ] THEIA platform
- [x] Demonstration and validation activities
- [x] Communication, Dissemination, Training and Exploitation
- [ ] Others

Q2.2. If Others, please specify which ones, and within which Work Package in the project.

None

Q2.3. Briefly describe the objectives and possible benefits of the development and use of the technology in the project.

Some of the developed tools could be further evolved and adapted to support geospatial intelligence activities linked with our core business.

Q3.1.
Are you processing or intend to process personal data when developing or using these technologies in THEIA?

Please keep in mind that the terms 'personal data' and 'processing' are rather broad. Processing means the use of personal data at any stage of the Project: collecting, recording, studying and publishing these data, amongst others. Personal data are any information relating to an identified or identifiable natural person. For instance, in THEIA: the processing of a dataset including footage with a camera that records people, the curation of intelligence data from publicly available sources or social media about individuals behaviour, or the collection of information from potential end-users that identify the counterparts, or interaction with them. All these activities imply the processing of personal data, and require an affirmative answer. On the other hand, processing datasets that solely include technical data about UAVs, satellites signal, or geo-spacial resources would not be considered processing of personal data. ***When in doubt, you generally process some personal data. If you have any questions about this, or do not exactly know if you process personal data, please contact MPlegal before continuing with the survey.***

- ○ Yes
- ◉ No

Q3.2.
Please specify the types of personal data which you process.

The categories below are provided for orientation and are not necessarily needed for the purposes of the project. Please specify those relevant to your activities.

This question was not displayed to the respondent.

Q3.3. Develop your previous answer, if it is necessary for any category, or if you clicked "Others".

This question was not displayed to the respondent.

Q3.4.
How will you obtain the personal data?

This question was not displayed to the respondent.

Q3.5. Please specify the sources and means of receiving with regards to all the categories of personal data.

This question was not displayed to the respondent.

Q3.6. Develop and classify per set of personal data the sources.

E.g. Identification data (name and email) are obtained directly from data subjects through a website. Biometric data (facial geometry) are obtained from existing datasets through

This question was not displayed to the respondent.

Q3.7. People need to be informed of the processing of their personal data, unless they are obtained indirecty or anonymised. How do you inform the data subject about the processing activity of personal data?

Please come back to MPlegal with any questions regarding this aspect.

This question was not displayed to the respondent.

Q3.8.
Whose personal data is being processed?

Please describe the data subjects, i.e., the individuals or groups of research participants whose personal data will be collected and processed during the project.

This question was not displayed to the respondent.

Q3.9.
How will you arrange the personal data?

Please describe the datasets of personal data that you have, and map basically your information flows (i.e. what data, where it comes from and where it goes – if it is within your organisation, mention the department; if outside, which partners. **This needs to be a basic answer, which will be developed and used as a base for developing a Data flow map in next deliverables for THEIA.**

This question was not displayed to the respondent.

Q3.10.

What do you want to achieve by collecting the personal data?

Please describe for all the categories of personal data.

This question was not displayed to the respondent.

Q3.11.
How will you use the personal data?

Please describe briefly and precisely for all the categories of personal data.

This question was not displayed to the respondent.

Q3.12.
Is the processing of the personal data really necessary to achieve your purpose?

This question was not displayed to the respondent.

Q3.13. Have you explored alternative means to the use of personal data? (mock data, anonymous dataset, fewer variables of personal data…) How satisfactory would they be to achieve the same outcome?

This question was not displayed to the respondent.

Q3.14.
Where will the personal data be stored?

Please explain the location

This question was not displayed to the respondent.

Q3.15. Where are these servers / storage of personal data?

This question was not displayed to the respondent.

Q3.16.
Will you share the datasets of personal data with third parties, not members of the THEIA consortium?

This question was not displayed to the respondent.

Q3.17.
If yes, please explain the reasons and name the receivers. Please specify if these receivers are located in the European Union or abroad.

This question was not displayed to the respondent.

Q3.18.
Will you cooperate with other partners or external entities for the processing of the personal data?

This question was not displayed to the respondent.

Q3.19.
***If yes**, please specify:*

This question was not displayed to the respondent.

Q3.20.
If you engage with other entities to assist you in data processing, what type of work do they develop? How do you make sure that they comply with data protection principles?
Please describe data types and purposes of joint processing.

This question was not displayed to the respondent.

Q3.21.
Will you work with an external online tool, or other cloud computing solution to process personal data?
If so, which one? Do you know the geographical location for storage of information of such tool or cloud servers (e.g. Europe, US, Canada, Japan)?

This question was not displayed to the respondent.

Q3.22.
In your view, do you think you will need to store the personal data collected for this project after its ending?

Could you please provide a justification, in the light of the purpose for which you process personal data?

This question was not displayed to the respondent.

Q3.23.
Would you be willing to anonymise the data?

Data anonymisation *is a process applied to personal data after which it is no longer possible, now, or in the future, to trace the identity of the individual. It is normally done by separating the elements in the dataset that allow identification. Or assigning random codes of identification to the datasets that cannot be traced back to the original data subject, through encryption.*

This question was not displayed to the respondent.

Q3.24.
***If no**, please provide the reasons.*

This question was not displayed to the respondent.

Q3.25.
Would you be willing to pseudonymise the data?

Pseudonymisation *is a process applied to personal data, replacing the identifiable parts of the dataset with a code or reference number, using an agreed upon code. If you need it, you can reverse the process, and obtain back the individual identity through the used code.*

This question was not displayed to the respondent.

Q3.26.
***If no**, please provide the reasons.*

This question was not displayed to the respondent.

Q3.27. Will you implement data protection by design and by default measures?

Some examples of these measures are providing the control to the data subject over his/her personal data once the technology is implemented. Or reduce the data needed and pseudonymise it.

This question was not displayed to the respondent.

Q3.28.
If yes, develop which ones**. If not**, please provide the reasons.

This question was not displayed to the respondent.

Q3.29.
Will your technology be used for profiling data subjects and/or take automated decisions based solely on the processing of personal data from the data subject? This includes, amongst others, feeding Artificial Intelligence models with the data, in order to obtain decisions over these data subjects.

This question was not displayed to the respondent.

Q3.30. If so, what kind of decisions?

This question was not displayed to the respondent.

Q3.31.
Do you follow or comply with any code of conduct or certification scheme in connection to the processing of personal data? For instance, ISO/IEC 27001:2022 standard for Information security, cybersecurity and privacy protection, Information security management systems; ISO/IEC 42005 Information technology — Artificial intelligence (AI) — AI system impact assessment, or the International Association of Privacy Professionals (IAPP) certifications.

This question was not displayed to the respondent.

Q3.32.
Please identify and provide, if possible, the document or link to the document of certification.

This question was not displayed to the respondent.

Q3.33.
What will be the measures that you will take to secure the personal data that you process?

This question was not displayed to the respondent.

Q3.34.

Data subjects have certain rights under European law regarding the use and processing of their personal data. Do you already have a structure to ensure that data subjects are able to exercise their data subjects rights?

Some examples of these are the right of access to their personal data collected for the purposes of the project, right to erasure such data, right to rectification, right to data portability, possibility for the data subject to withdraw consent. The canalisations of those requests through a Data Protection Officer could be an example of an existing structure.

This question was not displayed to the respondent.

Q3.35.
Please specify technical (e.g. specific email address for requests, software or in-built secure system allowing data subjects to access their own personal data in a transparent way) and organisational measures (e.g. who will provide the information to the data subject) to secure the personal data that you already put in place?

Will you need to limit those data subject rights? If so, please specify which one(s) and the reason to do so.

This question was not displayed to the respondent.

Q3.36. How large is the volume of personal data that you process in the project?

This question was not displayed to the respondent.

Q3.37. Do you process any personal data of children?

Meaning underage people, below the age of 16 years old.

This question was not displayed to the respondent.

Q3.38. Where do you obtain the personal data from children?

i.e. directly from them, from existing datasets, from their parents.

This question was not displayed to the respondent.

Q3.39. If you process personal data from minors, do you contact their parents/legal guardians? What information do you share with them about the data processing?

This question was not displayed to the respondent.

Q3.40. Are third parties involved in the processing of personal data?

This question was not displayed to the respondent.

Q3.41. Who are these third parties? What do they do with the personal data?

This question was not displayed to the respondent.

Q3.42. Please, justify your answer. For instance: we do not process personal data, because all the information that we use in the research project is technical data. Another cause will be that you access personal information, but you cannot identify individuals (anonymisation of personal data). Provide as many details as possible, and examples of the information.

We do not process personal data, because all the information that we use in the research project is technical data. Most of the data we used was based on vectors or satellite imagery, not containing any personal data.

Q4.1. Do you use existing datasets in your research in the project?

- (●) Yes
- ( ) No

Q4.2. What is the origin of the datasets?

- ( ) They were in our possesion before the start of the project.
- (●) They are publicly available.
- ( ) We obtained them after the start of the project free of cost.
- ( ) We obtained them after the start of the project with a licensing access commercial agreement.
- ( ) I do not know.

Q4.3. Do you consider that the datasets may include personal data in them? Please refer to the information in the previous questions from section 2 about personal data.

- ( ) Definitely yes. It is possible to identify individuals within the dataset.
- ( ) Definitely yes. The data are anonymised. There is personal information in the dataset, but it is not possible to identify the individual.
- ( ) Probably yes.
- ( ) Probably no.
- (●) Definitely no.

Q5.1.
Do you think the use or development of the technology might impact privacy of individuals? (such as migrants, including displaced population due to armed conflicts or climate change, minors, undocumented people, and refugees)

Please keep in mind that privacy might be affected without processing of personal data (for example, drones flying above a private house, satellites capturing metrics of properties and terrain). **If you have any questions about this, or do not exactly know if privacy may be impacted, please contact MPlegal before continuing with the survey.**

- ( ) Yes
- (●) No

◯ Maybe

Q5.2. How does your use or development of the technology potentially impact privacy of individuals?

This question was not displayed to the respondent.

Q5.3.
Is this impact on privacy adequate and necessary to achieve the purpose for the development of this technology? For instance, develop the mission and mandate of a public entity, or provide a technical-tool/research that cannot be developed in any other way.

This question was not displayed to the respondent.

Q5.4. Please explain why.

This question was not displayed to the respondent.

Q5.5.
Are there less invasive solutions that can be used to achieve the same purpose effectively?

This question was not displayed to the respondent.

Q5.6. If yes, which are they, and why are they not used?

This question was not displayed to the respondent.

Q5.7. Do you think the benefits which result from the 'adequate and necessary' (research) activity are higher than the impact that it will cause for the privacy of the user?

This question was not displayed to the respondent.

Q5.8. Please explain why.

This question was not displayed to the respondent.

Q5.9. Does the implementation or use of the technology affect the subjects moral, religious or cultural integrity?

This question was not displayed to the respondent.

Q6.1.
What would be, in your opinion, the benefit for the end-users of the technology and society?

State-of-the-art tools oriented to support law enforcement and authorities to tackle environmental crimes of different nature and origin.

Q6.2.
Are there possible safety risks for the subjects related to the use of the technology?

- ○ Yes
- ◉ No
- ○ There might be.

Q6.3. Please, describe them, or justify the negative answer. For instance: there are risks, but we foresee safeguards that reduce them.

Developed technologies are based on remote sensing, not considering them as suitable to generate safety risks for the subjects related to the use of that technology.

Q6.4.
What technical and organizational measures can be taken to ensure and increase safety of the technology for end-users and data subjects?

Limited used of the technology and for trained users only.

Q6.5. Are there any technical and organizational measures which could be taken to increase trust of the society and individuals in the use of the technology?

Promoting and openly presenting the developed technologies could bring a higher level of trust from the society.

Q6.6.
Do you foresee any ethical issues related to the development or use of the technology?

- ○ Yes
- ◉ No

Q6.7. Please describe them.

None

Q7.1. Are the data used in the project susceptible of misuse? Could they be used, once processed, in a harmful way for the Project or for society?

Such possibility is not foreseen at this stage.

Q7.2. Are there any measures already implemented which would prevent this misuse to happen?

- (●) Yes
- ( ) No

Q7.3. Detail them or suggest new ones that could be implemented.

Labelling some of the deliverables as sensitive is protecting some data and information to be shared with non-desired receptors.

Q8.1.
Are there any risks of stigmatisation or discrimination, to your knowledge, in the use of these technologies in GeoAI and law enforcement?

The use of data for law enforcement is a sensitive domain for the general public. Particularly, border surveillance and security raises many societal and ethical questions. The treatment at large scale of information about borders and personal data about migrants needs to be performed in a comprehensive, sensible and protected way. Security measures and responses must be tailored to consider the needs and of vulnerable groups. The potential risk of misinformation must also be considered, as well as the potential generation or amplification of harmful stereotypes concerning these vulnerable groups.

- ( ) Yes
- (●) No

Q8.2. Are there any direct risks of misinformation associated to the use of these technologies?

- ( ) Yes
- (●) No

Q8.3. If any of these risks is spotted, what is the procedure you would follow to minimise and correct the affected stigmatisation or discrimination?

Closely monitoring the detected risk and applying any necessary measure which in on our hands to eliminate it.

Q9.1. THEIA project has endeavoured to develop the research with attention to gender, inclusion, and adequate social norms. This requires not to consider, and not to inflict any negative gender stereotypes. The creation or propagation of gender stereotypes could lead to issues of discrimination for particular genders, or

worsen other problematic already existing, and potential discrimination. Could the use of the technology help in tackling these stereotypes?

- ○ Yes
- ◉ No

Q9.2. How does it do so?

Not in relation to the technology developed under this project.

Q9.3. Are there any risks of amplification of gender issues in the use of your technology, or development of your research in the project? Please describe them.

At the best of our knowledge, there is not such a risk at this stage.

Q10.1.
If you consider that an important point has not been asked or you would like to make a comment for feedback, please type it down here.

THANK YOU FOR ANSWERING THE QUESTIONS!

None

Q1.1. Which type of organisation do you represent in the Project?

- ○ End user
- ◉ Project partner
- ○ Stakeholder

Q1.2. Type-in the name of your organisation or the partner you represent in THEIA project

OHB Digital Services

Q1.3.
Please, type-in your name.

Your name will not be shared with anyone, neither with the other partners of the Consortium, nor published with the survey. It will only be used if internal checking of the results, or feedback is needed by MPLegal.

Q2.1.
Which technology or process is developed or used by your organisation in the project?

- ☐ Data processing pathway
- ☐ Users requirements coordination, demo activities and use-cases
- ☑ Very-High-Resolution Earth Observation tools (Thermal imaging and low-visibility sensing)
- ☐ Very-High-Resolution Earth Observation tools (Data acquisition: Space-based video)
- ☐ Very-High-Resolution Earth Observation tools (Data acquisition: Satellite-Based Multi-Payload Data)
- ☐ Data acquisition: Micro-satellites & Cubesats
- ☐ Data acquisition: UAS-based data
- ☐ Integration of the multi-sensor platform
- ☐ Testing sensors on drones. Drones deployment for testing in real conditions
- ☑ AI for detecting and tracking objects
- ☐ THEIA crowdsourcing tool
- ☐ Database for the Areas of Interest
- ☐ High-velocity transnational data
- ☐ Data fusion & Data models. Data exchange framework

- [ ] Data exchange platform for cloud infrastructure to satellite data
- [ ] National Constellation Data Federation
- [ ] Optimized API Access
- [ ] GeoAI. UAS and terrestrial sensor-based image processing
- [ ] GeoAI. Georeferencing
- [ ] GeoAI. Intelligence Gathering
- [x] GeoAI. Fusion and GeoAI Module
- [ ] THEIA platform
- [ ] Demonstration and validation activities
- [ ] Communication, Dissemination, Training and Exploitation
- [ ] Others

Q2.2. If Others, please specify which ones, and within which Work Package in the project.

Q2.3. Briefly describe the objectives and possible benefits of the development and use of the technology in the project.

Select suitable EO sources for THEIA use cases (WP6). Detect objects of interest in (those) satellite images. (WP10).

Q3.1.
Are you processing or intend to process personal data when developing or using these technologies in THEIA?

Please keep in mind that the terms 'personal data' and 'processing' are rather broad. Processing means the use of personal data at any stage of the Project: collecting, recording, studying and publishing these data, amongst others. Personal data are any information relating to an identified or identifiable natural person. For instance, in THEIA: the processing of a dataset including footage with a camera that records people, the curation of intelligence data from publicly available sources or social media about individuals behaviour, or the collection of information from potential end-users that identify the counterparts, or interaction with them. All these activities imply the processing of personal data, and require an affirmative answer. On the other hand, processing datasets that solely include technical data about UAVs, satellites signal, or geo-spacial resources would not be considered processing of personal data. ***When in doubt, you generally process some personal data. If you have any questions about this, or do not exactly know if you process personal data, please contact MPlegal before continuing with the survey.***

- ○ Yes
- ◉ No

Q3.2.
Please specify the types of personal data which you process.

The categories below are provided for orientation and are not necessarily needed for the purposes of the project. Please specify those relevant to your activities.

This question was not displayed to the respondent.

Q3.3. Develop your previous answer, if it is necessary for any category, or if you clicked "Others".

This question was not displayed to the respondent.

Q3.4.
How will you obtain the personal data?

This question was not displayed to the respondent.

Q3.5. Please specify the sources and means of receiving with regards to all the categories of personal data.

This question was not displayed to the respondent.

Q3.6. Develop and classify per set of personal data the sources.

E.g. Identification data (name and email) are obtained directly from data subjects through a website. Biometric data (facial geometry) are obtained from existing datasets through

This question was not displayed to the respondent.

Q3.7. People need to be informed of the processing of their personal data, unless they are obtained indirecty or anonymised. How do you inform the data subject about the processing activity of personal data?

Please come back to MPlegal with any questions regarding this aspect.

This question was not displayed to the respondent.

Q3.8.
Whose personal data is being processed?

Please describe the data subjects, i.e., the individuals or groups of research participants whose personal data will be collected and processed during the project.

This question was not displayed to the respondent.

Q3.9.
How will you arrange the personal data?

Please describe the datasets of personal data that you have, and map basically your information flows (i.e. what data, where it comes from and where it goes – if it is within your organisation, mention the department; if outside, which partners. **This needs to be a basic answer, which will be developed and used as a base for developing a Data flow map in next deliverables for THEIA.**

This question was not displayed to the respondent.

Q3.10.

What do you want to achieve by collecting the personal data?

Please describe for all the categories of personal data.

This question was not displayed to the respondent.

Q3.11.
How will you use the personal data?

Please describe briefly and precisely for all the categories of personal data.

This question was not displayed to the respondent.

Q3.12.
Is the processing of the personal data really necessary to achieve your purpose?

This question was not displayed to the respondent.

Q3.13. Have you explored alternative means to the use of personal data? (mock data, anonymous dataset, fewer variables of personal data…) How satisfactory would they be to achieve the same outcome?

This question was not displayed to the respondent.

Q3.14.
Where will the personal data be stored?

Please explain the location

This question was not displayed to the respondent.

Q3.15. Where are these servers / storage of personal data?

This question was not displayed to the respondent.

Q3.16.
Will you share the datasets of personal data with third parties, not members of the THEIA consortium?

This question was not displayed to the respondent.

Q3.17.
If yes, please explain the reasons and name the receivers. Please specify if these receivers are located in the European Union or abroad.

This question was not displayed to the respondent.

Q3.18.
Will you cooperate with other partners or external entities for the processing of the personal data?

This question was not displayed to the respondent.

Q3.19.
***If yes**, please specify:*

This question was not displayed to the respondent.

Q3.20.
If you engage with other entities to assist you in data processing, what type of work do they develop? How do you make sure that they comply with data protection principles?
Please describe data types and purposes of joint processing.

This question was not displayed to the respondent.

Q3.21.
Will you work with an external online tool, or other cloud computing solution to process personal data?
If so, which one? Do you know the geographical location for storage of information of such tool or cloud servers (e.g. Europe, US, Canada, Japan)?

This question was not displayed to the respondent.

Q3.22.
In your view, do you think you will need to store the personal data collected for this project after its ending?

Could you please provide a justification, in the light of the purpose for which you process personal data?

This question was not displayed to the respondent.

Q3.23.
Would you be willing to anonymise the data?

Data anonymisation *is a process applied to personal data after which it is no longer possible, now, or in the future, to trace the identity of the individual. It is normally done by separating the elements in the dataset that allow identification. Or assigning random codes of identification to the datasets that cannot be traced back to the original data subject, through encryption.*

This question was not displayed to the respondent.

Q3.24.
***If no**, please provide the reasons.*

This question was not displayed to the respondent.

Q3.25.
Would you be willing to pseudonymise the data?

Pseudonymisation *is a process applied to personal data, replacing the identifiable parts of the dataset with a code or reference number, using an agreed upon code. If you need it, you can reverse the process, and obtain back the individual identity through the used code.*

This question was not displayed to the respondent.

Q3.26.
***If no**, please provide the reasons.*

This question was not displayed to the respondent.

Q3.27. Will you implement data protection by design and by default measures?

Some examples of these measures are providing the control to the data subject over his/her personal data once the technology is implemented. Or reduce the data needed and pseudonymise it.

This question was not displayed to the respondent.

Q3.28.
If yes, develop which ones**. If not**, please provide the reasons.

This question was not displayed to the respondent.

Q3.29.
Will your technology be used for profiling data subjects and/or take automated decisions based solely on the processing of personal data from the data subject? This includes, amongst others, feeding Artificial Intelligence models with the data, in order to obtain decisions over these data subjects.

This question was not displayed to the respondent.

Q3.30. If so, what kind of decisions?

This question was not displayed to the respondent.

Q3.31.
Do you follow or comply with any code of conduct or certification scheme in connection to the processing of personal data? For instance, ISO/IEC 27001:2022 standard for Information security, cybersecurity and privacy protection, Information security management systems; ISO/IEC 42005 Information technology — Artificial intelligence (AI) — AI system impact assessment, or the International Association of Privacy Professionals (IAPP) certifications.

This question was not displayed to the respondent.

Q3.32.
Please identify and provide, if possible, the document or link to the document of certification.

This question was not displayed to the respondent.

Q3.33.
What will be the measures that you will take to secure the personal data that you process?

This question was not displayed to the respondent.

Q3.34.

Data subjects have certain rights under European law regarding the use and processing of their personal data. Do you already have a structure to ensure that data subjects are able to exercise their data subjects rights?

Some examples of these are the right of access to their personal data collected for the purposes of the project, right to erasure such data, right to rectification, right to data portability, possibility for the data subject to withdraw consent. The canalisations of those requests through a Data Protection Officer could be an example of an existing structure.

This question was not displayed to the respondent.

Q3.35.
Please specify technical (e.g. specific email address for requests, software or in-built secure system allowing data subjects to access their own personal data in a transparent way) and organisational measures (e.g. who will provide the information to the data subject) to secure the personal data that you already put in place?

Will you need to limit those data subject rights? If so, please specify which one(s) and the reason to do so.

This question was not displayed to the respondent.

Q3.36. How large is the volume of personal data that you process in the project?

This question was not displayed to the respondent.

Q3.37. Do you process any personal data of children?

Meaning underage people, below the age of 16 years old.

This question was not displayed to the respondent.

Q3.38. Where do you obtain the personal data from children?

i.e. directly from them, from existing datasets, from their parents.

This question was not displayed to the respondent.

Q3.39. If you process personal data from minors, do you contact their parents/legal guardians? What information do you share with them about the data processing?

This question was not displayed to the respondent.

Q3.40. Are third parties involved in the processing of personal data?

This question was not displayed to the respondent.

Q3.41. Who are these third parties? What do they do with the personal data?

This question was not displayed to the respondent.

Q3.42. Please, justify your answer. For instance: we do not process personal data, because all the information that we use in the research project is technical data. Another cause will be that you access personal information, but you cannot identify individuals (anonymisation of personal data). Provide as many details as possible, and examples of the information.

Satellite imagery only. The resolution does not allow the identification of individuals. . I really cannot think of anything more to say, but I have to reach 200 characters...

Q4.1. Do you use existing datasets in your research in the project?

- (●) Yes
- ( ) No

Q4.2. What is the origin of the datasets?

- ( ) They were in our possesion before the start of the project.
- (●) They are publicly available.
- ( ) We obtained them after the start of the project free of cost.
- ( ) We obtained them after the start of the project with a licensing access commercial agreement.
- ( ) I do not know.

Q4.3. Do you consider that the datasets may include personal data in them? Please refer to the information in the previous questions from section 2 about personal data.

- ( ) Definitely yes. It is possible to identify individuals within the dataset.
- ( ) Definitely yes. The data are anonymised. There is personal information in the dataset, but it is not possible to identify the individual.
- ( ) Probably yes.
- ( ) Probably no.
- (●) Definitely no.

Q5.1.
Do you think the use or development of the technology might impact privacy of individuals? (such as migrants, including displaced population due to armed conflicts or climate change, minors, undocumented people, and refugees)

Please keep in mind that privacy might be affected without processing of personal data (for example, drones flying above a private house, satellites capturing metrics of properties and terrain). **If you have any questions about this, or do not exactly know if privacy may be impacted, please contact MPlegal before continuing with the survey.**

- ( ) Yes
- (●) No

◯ Maybe

Q5.2. How does your use or development of the technology potentially impact privacy of individuals?

This question was not displayed to the respondent.

Q5.3.
Is this impact on privacy adequate and necessary to achieve the purpose for the development of this technology? For instance, develop the mission and mandate of a public entity, or provide a technical-tool/research that cannot be developed in any other way.

This question was not displayed to the respondent.

Q5.4. Please explain why.

This question was not displayed to the respondent.

Q5.5.
Are there less invasive solutions that can be used to achieve the same purpose effectively?

This question was not displayed to the respondent.

Q5.6. If yes, which are they, and why are they not used?

This question was not displayed to the respondent.

Q5.7. Do you think the benefits which result from the 'adequate and necessary' (research) activity are higher than the impact that it will cause for the privacy of the user?

This question was not displayed to the respondent.

Q5.8. Please explain why.

This question was not displayed to the respondent.

Q5.9. Does the implementation or use of the technology affect the subjects moral, religious or cultural integrity?

This question was not displayed to the respondent.

Q6.1.
What would be, in your opinion, the benefit for the end-users of the technology and society?

A few new tools in the tool box that bring us closer to: - using Very High Resolution Satellites for Civil Security on EU level. - coordinating Ground Sensors and UAVs on sensitive sites. - reacting fast to extreme events.

Q6.2.
Are there possible safety risks for the subjects related to the use of the technology?

- ○ Yes
- ○ No
- ◉ There might be.

Q6.3. Please, describe them, or justify the negative answer. For instance: there are risks, but we foresee safeguards that reduce them.

It depends on the use of the technology. It can be used to help and safeguard pepole during a crisis. However it can also be used to exacerbate inequality e.g. by tightening borders.

Q6.4.
What technical and organizational measures can be taken to ensure and increase safety of the technology for end-users and data subjects?

The mission given to the user is crutial and the metric by which they are evaluated.

Q6.5. Are there any technical and organizational measures which could be taken to increase trust of the society and individuals in the use of the technology?

Public transparency of the given user mission and metrics. Internal transparency of the user actions.

Q6.6.
Do you foresee any ethical issues related to the development or use of the technology?

- ◉ Yes
- ○ No

Q6.7. Please describe them.

Powerful surveillance tools do not do harm in and of themselves. Their application must be conducted ethically.

Q7.1. Are the data used in the project susceptible of misuse? Could they be used, once processed, in a harmful way for the Project or for society?

Most aspects of THEIA (ship, vehicle, and border traffic) are monitored and regulated anyway. Harm may be done if surveillance tools are abused by malicious actors. E.g. by tracking individulas in camera feeds.

Q7.2. Are there any measures already implemented which would prevent this misuse to happen?

- (●) Yes
- ( ) No

Q7.3. Detail them or suggest new ones that could be implemented.

Camera sensors would only be placed at sensitive public places like border crossings. Access to THEIA data may only be granted to trusted entities.

Q8.1.
Are there any risks of stigmatisation or discrimination, to your knowledge, in the use of these technologies in GeoAI and law enforcement?

The use of data for law enforcement is a sensitive domain for the general public. Particularly, border surveillance and security raises many societal and ethical questions. The treatment at large scale of information about borders and personal data about migrants needs to be performed in a comprehensive, sensible and protected way. Security measures and responses must be tailored to consider the needs and of vulnerable groups. The potential risk of misinformation must also be considered, as well as the potential generation or amplification of harmful stereotypes concerning these vulnerable groups.

- (●) Yes
- ( ) No

Q8.2. Are there any direct risks of misinformation associated to the use of these technologies?

- ( ) Yes
- (●) No

Q8.3. If any of these risks is spotted, what is the procedure you would follow to minimise and correct the affected stigmatisation or discrimination?

Stigmatisation may occur if e.g. refugees are viewed as a thread rather than human beigns in need. Detecting forced displacement must be tied to the aspiration to help rather than to deflect a problem.

Q9.1. THEIA project has endeavoured to develop the research with attention to gender, inclusion, and adequate social norms. This requires not to consider, and not to inflict any negative gender stereotypes. The creation or propagation of gender stereotypes could lead to issues of discrimination for particular genders, or

worsen other problematic already existing, and potential discrimination. Could the use of the technology help in tackling these stereotypes?

- ○ Yes
- ◉ No

Q9.2. How does it do so?

-

Q9.3. Are there any risks of amplification of gender issues in the use of your technology, or development of your research in the project? Please describe them.

-

Q10.1.
If you consider that an important point has not been asked or you would like to make a comment for feedback, please type it down here.

THANK YOU FOR ANSWERING THE QUESTIONS!

Q1.1. Which type of organisation do you represent in the Project?

- ○ End user
- ◉ Project partner
- ○ Stakeholder

Q1.2. Type-in the name of your organisation or the partner you represent in THEIA project

LuxSpace Sàrl

Q1.3.
Please, type-in your name.

Your name will not be shared with anyone, neither with the other partners of the Consortium, nor published with the survey. It will only be used if internal checking of the results, or feedback is needed by MPLegal.

Q2.1.
Which technology or process is developed or used by your organisation in the project?

- ☐ Data processing pathway
- ☑ Users requirements coordination, demo activities and use-cases
- ☐ Very-High-Resolution Earth Observation tools (Thermal imaging and low-visibility sensing)
- ☐ Very-High-Resolution Earth Observation tools (Data acquisition: Space-based video)
- ☐ Very-High-Resolution Earth Observation tools (Data acquisition: Satellite-Based Multi-Payload Data)
- ☑ Data acquisition: Micro-satellites & Cubesats
- ☐ Data acquisition: UAS-based data
- ☐ Integration of the multi-sensor platform
- ☐ Testing sensors on drones. Drones deployment for testing in real conditions
- ☑ AI for detecting and tracking objects
- ☐ THEIA crowdsourcing tool
- ☐ Database for the Areas of Interest
- ☐ High-velocity transnational data
- ☑ Data fusion & Data models. Data exchange framework

- [ ] Data exchange platform for cloud infrastructure to satellite data
- [ ] National Constellation Data Federation
- [ ] Optimized API Access
- [ ] GeoAI. UAS and terrestrial sensor-based image processing
- [ ] GeoAI. Georeferencing
- [ ] GeoAI. Intelligence Gathering
- [x] GeoAI. Fusion and GeoAI Module
- [ ] THEIA platform
- [ ] Demonstration and validation activities
- [ ] Communication, Dissemination, Training and Exploitation
- [x] Others

Q2.2. If Others, please specify which ones, and within which Work Package in the project.

Data acquisition: RF and analytics (probably integrated in the Micro-satellites & Cubesats, but it describes better the presence of RF data within the project) - it is included in the Data acquisition: Microsatellites & CubeSats, but I think it deserves a different category. We are also not directly involved in other processes like VHR missions (some of the screened missions in WP7 are also in WP6, so we are frequently exchanging some info). Also since we are developing some processes/technology (object detection tool) it will be also integrated in the THEIA platform - therefore we are also indirectly involved in this and potentially in the demo and validation activities (not marked as only indirectly involved)

Q2.3. Briefly describe the objectives and possible benefits of the development and use of the technology in the project.

THEIA will incorporate a rich set of data sources from a varied group of missisions and phenomenologies together with leading analytical tools--such as object detection, data fusion, route prediction, and multi-int object identification--to to create an innovative geospatial intelligence platform supporting and strenghthening mission users of the Copernicus Security Service. The end-result benefits will be quicker, better informed, and greater confidence decision-making in responding to population displacements which will result in better outcomes not only for the migrants or other displaced population groups, but also to a safer and more proactive environment for all EU Member State nationals and residents.

Q3.1.
Are you processing or intend to process personal data when developing or using these technologies in THEIA?

Please keep in mind that the terms 'personal data' and 'processing' are rather broad. Processing means the use of personal data at any stage of the Project: collecting, recording, studying and publishing these data, amongst others. Personal data are any information relating to an identified or identifiable natural person. For instance, in THEIA: the processing of a dataset including footage with a camera that records people, the curation of intelligence data from publicly available sources or social media about individuals behaviour, or the collection of information from potential end-users that identify the counterparts, or interaction with them. All these activities imply the processing of personal data, and require an affirmative answer. On the other hand, processing datasets that solely include technical data about UAVs, satellites signal, or geo-spacial resources would not be considered processing of personal data. ***When in doubt, you generally process some personal data. If you have any questions about this, or do not exactly know if you process personal data, please contact MPlegal before continuing with the survey.***

- ( ) Yes
- (•) No

Q3.2.
Please specify the types of personal data which you process.

The categories below are provided for orientation and are not necessarily needed for the purposes of the project. Please specify those relevant to your activities.

This question was not displayed to the respondent.

Q3.3. Develop your previous answer, if it is necessary for any category, or if you clicked "Others".

This question was not displayed to the respondent.

Q3.4.
How will you obtain the personal data?

This question was not displayed to the respondent.

Q3.5. Please specify the sources and means of receiving with regards to all the categories of personal data.

This question was not displayed to the respondent.

Q3.6. Develop and classify per set of personal data the sources.

E.g. Identification data (name and email) are obtained directly from data subjects through a website. Biometric data (facial geometry) are obtained from existing datasets through

This question was not displayed to the respondent.

Q3.7. People need to be informed of the processing of their personal data, unless they are obtained indirecty or anonymised. How do you inform the data subject about the processing activity of personal data?

Please come back to MPlegal with any questions regarding this aspect.

This question was not displayed to the respondent.

Q3.8.
Whose personal data is being processed?

Please describe the data subjects, i.e., the individuals or groups of research participants whose personal data will be collected and processed during the project.

This question was not displayed to the respondent.

Q3.9.
How will you arrange the personal data?

Please describe the datasets of personal data that you have, and map basically your information flows (i.e. what data, where it comes from and where it goes – if it is within your organisation, mention the department; if outside, which partners. **This needs to be a basic answer, which will be developed and used as a base for developing a Data flow map in next deliverables for THEIA.**

This question was not displayed to the respondent.

Q3.10.
What do you want to achieve by collecting the personal data?

Please describe for all the categories of personal data.

This question was not displayed to the respondent.

Q3.11.
How will you use the personal data?

Please describe briefly and precisely for all the categories of personal data.

This question was not displayed to the respondent.

Q3.12.
Is the processing of the personal data really necessary to achieve your purpose?

This question was not displayed to the respondent.

Q3.13. Have you explored alternative means to the use of personal data? (mock data, anonymous dataset, fewer variables of personal data…) How satisfactory would they be to achieve the same outcome?

This question was not displayed to the respondent.

Q3.14.
Where will the personal data be stored?

Please explain the location

This question was not displayed to the respondent.

Q3.15. Where are these servers / storage of personal data?

This question was not displayed to the respondent.

Q3.16.
Will you share the datasets of personal data with third parties, not members of the THEIA consortium?

This question was not displayed to the respondent.

Q3.17.
If yes, please explain the reasons and name the receivers. Please specify if these receivers are located in the European Union or abroad.

This question was not displayed to the respondent.

Q3.18.
Will you cooperate with other partners or external entities for the processing of the personal data?

This question was not displayed to the respondent.

Q3.19.
***If yes**, please specify:*

This question was not displayed to the respondent.

Q3.20.
If you engage with other entities to assist you in data processing, what type of work do they develop? How do you make sure that they comply with data protection principles?
Please describe data types and purposes of joint processing.

This question was not displayed to the respondent.

Q3.21.
Will you work with an external online tool, or other cloud computing solution to process personal data?
If so, which one? Do you know the geographical location for storage of information of such tool or cloud servers (e.g. Europe, US, Canada, Japan)?

This question was not displayed to the respondent.

Q3.22.
In your view, do you think you will need to store the personal data collected for this project after its ending?

Could you please provide a justification, in the light of the purpose for which you process personal data?

This question was not displayed to the respondent.

Q3.23.
Would you be willing to anonymise the data?

Data anonymisation *is a process applied to personal data after which it is no longer possible, now, or in the future, to trace the identity of the individual. It is normally done by separating the elements in the dataset that allow identification. Or assigning random codes of identification to the datasets that cannot be traced back to the original data subject, through encryption.*

This question was not displayed to the respondent.

Q3.24.
***If no**, please provide the reasons.*

This question was not displayed to the respondent.

Q3.25.
Would you be willing to pseudonymise the data?

Pseudonymisation *is a process applied to personal data, replacing the identifiable parts of the dataset with a code or reference number, using an agreed upon code. If you need it, you can reverse the process, and obtain back the individual identity through the used code.*

This question was not displayed to the respondent.

Q3.26.
***If no**, please provide the reasons.*

This question was not displayed to the respondent.

Q3.27. Will you implement data protection by design and by default measures?

Some examples of these measures are providing the control to the data subject over his/her personal data once the technology is implemented. Or reduce the data needed and pseudonymise it.

This question was not displayed to the respondent.

Q3.28.
If yes, develop which ones**. If not**, please provide the reasons.

This question was not displayed to the respondent.

Q3.29.
Will your technology be used for profiling data subjects and/or take automated decisions based solely on the processing of personal data from the data subject? This includes, amongst others, feeding Artificial Intelligence models with the data, in order to obtain decisions over these data subjects.

This question was not displayed to the respondent.

Q3.30. If so, what kind of decisions?

This question was not displayed to the respondent.

Q3.31.
Do you follow or comply with any code of conduct or certification scheme in connection to the processing of personal data? For instance, ISO/IEC 27001:2022 standard for Information security, cybersecurity and privacy protection, Information security management systems; ISO/IEC 42005 Information technology — Artificial intelligence (AI) — AI system impact assessment, or the International Association of Privacy Professionals (IAPP) certifications.

This question was not displayed to the respondent.

Q3.32.
Please identify and provide, if possible, the document or link to the document of certification.

This question was not displayed to the respondent.

Q3.33.
What will be the measures that you will take to secure the personal data that you process?

This question was not displayed to the respondent.

Q3.34.
Data subjects have certain rights under European law regarding the use and processing of their personal data. Do you already have a structure to ensure that data subjects are able to exercise their data subjects rights?

Some examples of these are the right of access to their personal data collected for the purposes of the project, right to erasure such data, right to rectification, right to data portability, possibility for the data subject to withdraw consent. The canalisations of those requests through a Data Protection Officer could be an example of an existing structure.

This question was not displayed to the respondent.

Q3.35.
Please specify technical (e.g. specific email address for requests, software or in-built secure system allowing data subjects to access their own personal data in a transparent way) and organisational measures (e.g. who will provide the information to the data subject) to secure the personal data that you already put in place?

Will you need to limit those data subject rights? If so, please specify which one(s) and the reason to do so.

This question was not displayed to the respondent.

Q3.36. How large is the volume of personal data that you process in the project?

This question was not displayed to the respondent.

Q3.37. Do you process any personal data of children?

Meaning underage people, below the age of 16 years old.

This question was not displayed to the respondent.

Q3.38. Where do you obtain the personal data from children?

i.e. directly from them, from existing datasets, from their parents.

This question was not displayed to the respondent.

Q3.39. If you process personal data from minors, do you contact their parents/legal guardians? What information do you share with them about the data processing?

This question was not displayed to the respondent.

Q3.40. Are third parties involved in the processing of personal data?

This question was not displayed to the respondent.

Q3.41. Who are these third parties? What do they do with the personal data?

This question was not displayed to the respondent.

Q3.42. Please, justify your answer. For instance: we do not process personal data, because all the information that we use in the research project is technical data. Another cause will be that you access personal information, but you cannot identify individuals (anonymisation of personal data). Provide as many details as possible, and examples of the information.

We do not process any personal data - within our tasks we work with different datasets but any of them will directly allow to identify individual: - We screen EO missions and use some datasets (Sentinel 1, Sentinel 2 and from other EO providers) where identification of individuals is not possible. - We screen RF missions and use some datasets (Unseelabs - requested but not yet received, but so far no personal information expected) From them we expect to get: georeferenced and dated location, emitters' technical parameters (usually parameters such as Frequency, signal accuracy level, pulses duration and repetition). However, we need first to get Unseenlabs data to be really sure that it is like this. Even if we even get the fingerprint of an emitter (we don't know yet if we will get this) it won't be possible to directly identify individuals with it. Also, and as well on RF data regard, the UR01 from D5.1 indicates that "the system (THEIA Platform) receives only the RF detection signal (including timestamp and location) and not caption of transmitted messages". Therefore, the information that we will use will focus only on signal detection. - Other datasets that we will use for the project purpose are AIS data, provided by LuxSpace commercial AIS service OrbitSailor.

Q4.1. Do you use existing datasets in your research in the project?

- (●) Yes
- ( ) No

Q4.2. What is the origin of the datasets?

- (●) They were in our possesion before the start of the project.
- ( ) They are publicly available.
- ( ) We obtained them after the start of the project free of cost.
- ( ) We obtained them after the start of the project with a licensing access commercial agreement.
- ( ) I do not know.

Q4.3. Do you consider that the datasets may include personal data in them? Please refer to the information in the previous questions from section 2 about personal data.

- ( ) Definitely yes. It is possible to identify individuals within the dataset.
- ( ) Definitely yes. The data are anonymised. There is personal information in the dataset, but it is not possible to identify the individual.
- ( ) Probably yes.
- (●) Probably no.
- ( ) Definitely no.

Q5.1.
Do you think the use or development of the technology might impact privacy of individuals? (such as migrants, including displaced population due to armed conflicts or climate change, minors, undocumented people, and refugees)

Please keep in mind that privacy might be affected without processing of personal data (for example, drones flying above a private house, satellites capturing metrics of properties and terrain). **If you have any**

questions about this, or do not exactly know if privacy may be impacted, please contact MPlegal before continuing with the survey.

- ○ Yes
- ◉ No
- ○ Maybe

Q5.2. How does your use or development of the technology potentially impact privacy of individuals?

This question was not displayed to the respondent.

Q5.3.
Is this impact on privacy adequate and necessary to achieve the purpose for the development of this technology? For instance, develop the mission and mandate of a public entity, or provide a technical-tool/research that cannot be developed in any other way.

This question was not displayed to the respondent.

Q5.4. Please explain why.

This question was not displayed to the respondent.

Q5.5.
Are there less invasive solutions that can be used to achieve the same purpose effectively?

This question was not displayed to the respondent.

Q5.6. If yes, which are they, and why are they not used?

This question was not displayed to the respondent.

Q5.7. Do you think the benefits which result from the 'adequate and necessary' (research) activity are higher than the impact that it will cause for the privacy of the user?

This question was not displayed to the respondent.

Q5.8. Please explain why.

This question was not displayed to the respondent.

Q5.9. Does the implementation or use of the technology affect the subjects moral, religious or cultural integrity?

This question was not displayed to the respondent.

Q6.1.
What would be, in your opinion, the benefit for the end-users of the technology and society?

With the intended end-users being european and Member State national defence, law enforcement, and search-and-rescue agencies (i.e., Copernicus Security Service users), the primary benefit of THEIA will be faster and more varied access to fused data and analytical products and alerts leading to quicker, better informed, and greater confidence decision-making in responding to population displacements which will result in better outcomes not only for the migrants or other displaced population groups, but also to a safer and more proactive environment for all EU Member State nationals and residents.

Q6.2.
Are there possible safety risks for the subjects related to the use of the technology?

- ○ Yes
- ◉ No
- ○ There might be.

Q6.3. Please, describe them, or justify the negative answer. For instance: there are risks, but we foresee safeguards that reduce them.

We do not forsee any risk for the users directly coming from the technology developed in THEIA. It may depend on the use the end-users give to it, but up to THEIA the purpose is only to identify objects / vehicles that implies people displacement due to different type of events.

Q6.4.
What technical and organizational measures can be taken to ensure and increase safety of the technology for end-users and data subjects?

Ensure that third-party providers meet security standards (for example - for RF, that only geolocation and location of the emitter is necessary) Strong access controls to the platform (only certain users having access), regular security testing (to avoid any interference)

Q6.5. Are there any technical and organizational measures which could be taken to increase trust of the society and individuals in the use of the technology?

The system can be designed to collect only the minimum amount of data necessary for operational purposes (avoiding doubts regarding to individual data privacy) Ensure that any personal data is anonymized Clear data-retention limits, audit logs, and strict access controls to the tool Transparent communication to society about the purpose of the system, the safeguards that are in place, and the types of data that are or are not collected Communicate that users are trained in privacy, ethics, and proportional use of the technology

Q6.6.
Do you foresee any ethical issues related to the development or use of the technology?

- ○ Yes
- ◉ No

Q6.7. Please describe them.

N/A

Q7.1. Are the data used in the project susceptible of misuse? Could they be used, once processed, in a harmful way for the Project or for society?

The data use need to follow EU regulation, therefore if this is controlled we do not foresee any potential misuse of the data and its products. End users belong to EU or national administrations or agencies, therefore they are subject of EU controls / audits, etc.

Q7.2. Are there any measures already implemented which would prevent this misuse to happen?

- (●) Yes
- ( ) No

Q7.3. Detail them or suggest new ones that could be implemented.

EU / national regulation

Q8.1.
Are there any risks of stigmatisation or discrimination, to your knowledge, in the use of these technologies in GeoAI and law enforcement?

The use of data for law enforcement is a sensitive domain for the general public. Particularly, border surveillance and security raises many societal and ethical questions. The treatment at large scale of information about borders and personal data about migrants needs to be performed in a comprehensive, sensible and protected way. Security measures and responses must be tailored to consider the needs and of vulnerable groups. The potential risk of misinformation must also be considered, as well as the potential generation or amplification of harmful stereotypes concerning these vulnerable groups.

- (●) Yes
- ( ) No

Q8.2. Are there any direct risks of misinformation associated to the use of these technologies?

- (●) Yes
- ( ) No

Q8.3. If any of these risks is spotted, what is the procedure you would follow to minimise and correct the affected stigmatisation or discrimination?

Would be good to regularly review the THEIA platform`s outputs to detect disproportionate impacts on specific areas or groups, investigating the causes of such patterns, and adjusting or retraining the model to remove biased behaviors (if detected). Human oversight, users training, and documentation of decisions may help to prevent misuse or over-reliance on automated outputs that would lead to stigmatisation or discrimination.

Q9.1. THEIA project has endeavoured to develop the research with attention to gender, inclusion, and adequate social norms. This requires not to consider, and not to inflict any negative gender stereotypes. The creation or propagation of gender stereotypes could lead to issues of discrimination for particular genders, or worsen other problematic already existing, and potential discrimination. Could the use of the technology help in tackling these stereotypes?

- ○ Yes
- ◉ No

Q9.2. How does it do so?

N/A

Q9.3. Are there any risks of amplification of gender issues in the use of your technology, or development of your research in the project? Please describe them.

Not that we are aware

Q10.1.
If you consider that an important point has not been asked or you would like to make a comment for feedback, please type it down here.

THANK YOU FOR ANSWERING THE QUESTIONS!

If you have any question regarding our answers, please do not hesitate contacting us anytime. Some of them may have been a bit general, in case more detail is required or it is felt some of the questions were not correctly understood, we will be happy to rectify the answer to make them more accurate. Thank you

Q1.1. Which type of organisation do you represent in the Project?

- ○ End user
- ◉ Project partner
- ○ Stakeholder

Q1.2. Type-in the name of your organisation or the partner you represent in THEIA project

ICCS

Q1.3.
Please, type-in your name.

Your name will not be shared with anyone, neither with the other partners of the Consortium, nor published with the survey. It will only be used if internal checking of the results, or feedback is needed by MPLegal.

Q2.1.
Which technology or process is developed or used by your organisation in the project?

- ☑ Data processing pathway
- ☐ Users requirements coordination, demo activities and use-cases
- ☑ Very-High-Resolution Earth Observation tools (Thermal imaging and low-visibility sensing)
- ☑ Very-High-Resolution Earth Observation tools (Data acquisition: Space-based video)
- ☑ Very-High-Resolution Earth Observation tools (Data acquisition: Satellite-Based Multi-Payload Data)
- ☐ Data acquisition: Micro-satellites & Cubesats
- ☐ Data acquisition: UAS-based data
- ☐ Integration of the multi-sensor platform
- ☐ Testing sensors on drones. Drones deployment for testing in real conditions
- ☑ AI for detecting and tracking objects
- ☐ THEIA crowdsourcing tool
- ☐ Database for the Areas of Interest
- ☐ High-velocity transnational data
- ☑ Data fusion & Data models. Data exchange framework

- [ ] Data exchange platform for cloud infrastructure to satellite data
- [ ] National Constellation Data Federation
- [ ] Optimized API Access
- [x] GeoAI. UAS and terrestrial sensor-based image processing
- [x] GeoAI. Georeferencing
- [x] GeoAI. Intelligence Gathering
- [x] GeoAI. Fusion and GeoAI Module
- [x] THEIA platform
- [ ] Demonstration and validation activities
- [ ] Communication, Dissemination, Training and Exploitation
- [ ] Others

Q2.2. If Others, please specify which ones, and within which Work Package in the project.

Q2.3. Briefly describe the objectives and possible benefits of the development and use of the technology in the project.

The development of THEIA Data Cubes framework and GeoAI algorithms can help on generating harmonized and homogeneous products, ready-to-use, that can help both the consortium partners and end-user on their advanced applications and decision making.

Q3.1.
Are you processing or intend to process personal data when developing or using these technologies in THEIA?

Please keep in mind that the terms 'personal data' and 'processing' are rather broad. Processing means the use of personal data at any stage of the Project: collecting, recording, studying and publishing these data, amongst others. Personal data are any information relating to an identified or identifiable natural person. For instance, in THEIA: the processing of a dataset including footage with a camera that records people, the curation of intelligence data from publicly available sources or social media about individuals behaviour, or the collection of information from potential end-users that identify the counterparts, or interaction with them. All these activities imply the processing of personal data, and require an affirmative answer. On the other hand, processing datasets that solely include technical data about UAVs, satellites signal, or geo-spacial resources would not be considered processing of personal data. ***When in doubt, you generally process some personal data. If you have any questions about this, or do not exactly know if you process personal data, please contact MPlegal before continuing with the survey.***

- ○ Yes
- ◉ No

Q3.2.
Please specify the types of personal data which you process.

The categories below are provided for orientation and are not necessarily needed for the purposes of the project. Please specify those relevant to your activities.

This question was not displayed to the respondent.

Q3.3. Develop your previous answer, if it is necessary for any category, or if you clicked "Others".

This question was not displayed to the respondent.

Q3.4.
How will you obtain the personal data?

This question was not displayed to the respondent.

Q3.5. Please specify the sources and means of receiving with regards to all the categories of personal data.

This question was not displayed to the respondent.

Q3.6. Develop and classify per set of personal data the sources.

E.g. Identification data (name and email) are obtained directly from data subjects through a website. Biometric data (facial geometry) are obtained from existing datasets through

This question was not displayed to the respondent.

Q3.7. People need to be informed of the processing of their personal data, unless they are obtained indirecty or anonymised. How do you inform the data subject about the processing activity of personal data?

Please come back to MPlegal with any questions regarding this aspect.

This question was not displayed to the respondent.

Q3.8.
Whose personal data is being processed?

Please describe the data subjects, i.e., the individuals or groups of research participants whose personal data will be collected and processed during the project.

This question was not displayed to the respondent.

Q3.9.
How will you arrange the personal data?

Please describe the datasets of personal data that you have, and map basically your information flows (i.e. what data, where it comes from and where it goes – if it is within your organisation, mention the department; if outside, which partners. **This needs to be a basic answer, which will be developed and used as a base for developing a Data flow map in next deliverables for THEIA.**

This question was not displayed to the respondent.

Q3.10.

What do you want to achieve by collecting the personal data?

Please describe for all the categories of personal data.

This question was not displayed to the respondent.

Q3.11.
How will you use the personal data?

Please describe briefly and precisely for all the categories of personal data.

This question was not displayed to the respondent.

Q3.12.
Is the processing of the personal data really necessary to achieve your purpose?

This question was not displayed to the respondent.

Q3.13. Have you explored alternative means to the use of personal data? (mock data, anonymous dataset, fewer variables of personal data…) How satisfactory would they be to achieve the same outcome?

This question was not displayed to the respondent.

Q3.14.
Where will the personal data be stored?

Please explain the location

This question was not displayed to the respondent.

Q3.15. Where are these servers / storage of personal data?

This question was not displayed to the respondent.

Q3.16.
Will you share the datasets of personal data with third parties, not members of the THEIA consortium?

This question was not displayed to the respondent.

Q3.17.
If yes, please explain the reasons and name the receivers. Please specify if these receivers are located in the European Union or abroad.

This question was not displayed to the respondent.

Q3.18.
Will you cooperate with other partners or external entities for the processing of the personal data?

This question was not displayed to the respondent.

Q3.19.
***If yes**, please specify:*

This question was not displayed to the respondent.

Q3.20.
If you engage with other entities to assist you in data processing, what type of work do they develop? How do you make sure that they comply with data protection principles?
Please describe data types and purposes of joint processing.

This question was not displayed to the respondent.

Q3.21.
Will you work with an external online tool, or other cloud computing solution to process personal data?
If so, which one? Do you know the geographical location for storage of information of such tool or cloud servers (e.g. Europe, US, Canada, Japan)?

This question was not displayed to the respondent.

Q3.22.
In your view, do you think you will need to store the personal data collected for this project after its ending?

Could you please provide a justification, in the light of the purpose for which you process personal data?

This question was not displayed to the respondent.

Q3.23.
Would you be willing to anonymise the data?

Data anonymisation *is a process applied to personal data after which it is no longer possible, now, or in the future, to trace the identity of the individual. It is normally done by separating the elements in the dataset that allow identification. Or assigning random codes of identification to the datasets that cannot be traced back to the original data subject, through encryption.*

This question was not displayed to the respondent.

Q3.24.
***If no**, please provide the reasons.*

This question was not displayed to the respondent.

Q3.25.
Would you be willing to pseudonymise the data?

Pseudonymisation *is a process applied to personal data, replacing the identifiable parts of the dataset with a code or reference number, using an agreed upon code. If you need it, you can reverse the process, and obtain back the individual identity through the used code.*

This question was not displayed to the respondent.

Q3.26.
***If no**, please provide the reasons.*

This question was not displayed to the respondent.

Q3.27. Will you implement data protection by design and by default measures?

Some examples of these measures are providing the control to the data subject over his/her personal data once the technology is implemented. Or reduce the data needed and pseudonymise it.

This question was not displayed to the respondent.

Q3.28.
If yes, develop which ones**. If not**, please provide the reasons.

This question was not displayed to the respondent.

Q3.29.
Will your technology be used for profiling data subjects and/or take automated decisions based solely on the processing of personal data from the data subject? This includes, amongst others, feeding Artificial Intelligence models with the data, in order to obtain decisions over these data subjects.

This question was not displayed to the respondent.

Q3.30. If so, what kind of decisions?

This question was not displayed to the respondent.

Q3.31.
Do you follow or comply with any code of conduct or certification scheme in connection to the processing of personal data? For instance, ISO/IEC 27001:2022 standard for Information security, cybersecurity and privacy protection, Information security management systems; ISO/IEC 42005 Information technology — Artificial intelligence (AI) — AI system impact assessment, or the International Association of Privacy Professionals (IAPP) certifications.

This question was not displayed to the respondent.

Q3.32.
Please identify and provide, if possible, the document or link to the document of certification.

This question was not displayed to the respondent.

Q3.33.
What will be the measures that you will take to secure the personal data that you process?

This question was not displayed to the respondent.

Q3.34.

Data subjects have certain rights under European law regarding the use and processing of their personal data. Do you already have a structure to ensure that data subjects are able to exercise their data subjects rights?

Some examples of these are the right of access to their personal data collected for the purposes of the project, right to erasure such data, right to rectification, right to data portability, possibility for the data subject to withdraw consent. The canalisations of those requests through a Data Protection Officer could be an example of an existing structure.

This question was not displayed to the respondent.

Q3.35.
Please specify technical (e.g. specific email address for requests, software or in-built secure system allowing data subjects to access their own personal data in a transparent way) and organisational measures (e.g. who will provide the information to the data subject) to secure the personal data that you already put in place?

Will you need to limit those data subject rights? If so, please specify which one(s) and the reason to do so.

This question was not displayed to the respondent.

Q3.36. How large is the volume of personal data that you process in the project?

This question was not displayed to the respondent.

Q3.37. Do you process any personal data of children?

Meaning underage people, below the age of 16 years old.

This question was not displayed to the respondent.

Q3.38. Where do you obtain the personal data from children?

i.e. directly from them, from existing datasets, from their parents.

This question was not displayed to the respondent.

Q3.39. If you process personal data from minors, do you contact their parents/legal guardians? What information do you share with them about the data processing?

This question was not displayed to the respondent.

Q3.40. Are third parties involved in the processing of personal data?

This question was not displayed to the respondent.

Q3.41. Who are these third parties? What do they do with the personal data?

This question was not displayed to the respondent.

Q3.42. Please, justify your answer. For instance: we do not process personal data, because all the information that we use in the research project is technical data. Another cause will be that you access personal information, but you cannot identify individuals (anonymisation of personal data). Provide as many details as possible, and examples of the information.

We do not process personal data under the Tasks of THEIA project. We implement GeoAI algorithms. If by any case any individual exists in any of the images/videos processed by these algorithms, this/these individual(s) will be anonymized and there will be no way to identify this/these individual(s).

Q4.1. Do you use existing datasets in your research in the project?

- (●) Yes
- ( ) No

Q4.2. What is the origin of the datasets?

- ( ) They were in our possesion before the start of the project.
- (●) They are publicly available.
- ( ) We obtained them after the start of the project free of cost.
- ( ) We obtained them after the start of the project with a licensing access commercial agreement.
- ( ) I do not know.

Q4.3. Do you consider that the datasets may include personal data in them? Please refer to the information in the previous questions from section 2 about personal data.

- ( ) Definitely yes. It is possible to identify individuals within the dataset.
- ( ) Definitely yes. The data are anonymised. There is personal information in the dataset, but it is not possible to identify the individual.
- ( ) Probably yes.
- (●) Probably no.
- ( ) Definitely no.

Q5.1.
Do you think the use or development of the technology might impact privacy of individuals? (such as migrants, including displaced population due to armed conflicts or climate change, minors, undocumented people, and refugees)

Please keep in mind that privacy might be affected without processing of personal data (for example, drones flying above a private house, satellites capturing metrics of properties and terrain). **If you have any questions about this, or do not exactly know if privacy may be impacted, please contact MPlegal before continuing with the survey.**

- ( ) Yes
- (●) No

◯ Maybe

Q5.2. How does your use or development of the technology potentially impact privacy of individuals?

This question was not displayed to the respondent.

Q5.3.
Is this impact on privacy adequate and necessary to achieve the purpose for the development of this technology? For instance, develop the mission and mandate of a public entity, or provide a technical-tool/research that cannot be developed in any other way.

This question was not displayed to the respondent.

Q5.4. Please explain why.

This question was not displayed to the respondent.

Q5.5.
Are there less invasive solutions that can be used to achieve the same purpose effectively?

This question was not displayed to the respondent.

Q5.6. If yes, which are they, and why are they not used?

This question was not displayed to the respondent.

Q5.7. Do you think the benefits which result from the 'adequate and necessary' (research) activity are higher than the impact that it will cause for the privacy of the user?

This question was not displayed to the respondent.

Q5.8. Please explain why.

This question was not displayed to the respondent.

Q5.9. Does the implementation or use of the technology affect the subjects moral, religious or cultural integrity?

This question was not displayed to the respondent.

Q6.1.
What would be, in your opinion, the benefit for the end-users of the technology and society?

The end users will have ready to use data for EO applications.

Q6.2.
Are there possible safety risks for the subjects related to the use of the technology?

- ○ Yes
- ◉ No
- ○ There might be.

Q6.3. Please, describe them, or justify the negative answer. For instance: there are risks, but we foresee safeguards that reduce them.

There are no safety risks in the developed EO technologies.

Q6.4.
What technical and organizational measures can be taken to ensure and increase safety of the technology for end-users and data subjects?

Q6.5. Are there any technical and organizational measures which could be taken to increase trust of the society and individuals in the use of the technology?

Q6.6.
Do you foresee any ethical issues related to the development or use of the technology?

- ○ Yes
- ◉ No

Q6.7. Please describe them.

Q7.1. Are the data used in the project susceptible of misuse? Could they be used, once processed, in a harmful way for the Project or for society?

The data are EO products open available from USGS and Copernicus services, thus these data cannot be misused.

Q7.2. Are there any measures already implemented which would prevent this misuse to happen?

- ○ Yes
- ◉ No

Q7.3. Detail them or suggest new ones that could be implemented.

Q8.1.
Are there any risks of stigmatisation or discrimination, to your knowledge, in the use of these technologies in GeoAI and law enforcement?

The use of data for law enforcement is a sensitive domain for the general public. Particularly, border surveillance and security raises many societal and ethical questions. The treatment at large scale of information about borders and personal data about migrants needs to be performed in a comprehensive, sensible and protected way. Security measures and responses must be tailored to consider the needs and of vulnerable groups. The potential risk of misinformation must also be considered, as well as the potential generation or amplification of harmful stereotypes concerning these vulnerable groups.

- ○ Yes
- ◉ No

Q8.2. Are there any direct risks of misinformation associated to the use of these technologies?

- ○ Yes
- ◉ No

Q8.3. If any of these risks is spotted, what is the procedure you would follow to minimise and correct the affected stigmatisation or discrimination?

Q9.1. THEIA project has endeavoured to develop the research with attention to gender, inclusion, and adequate social norms. This requires not to consider, and not to inflict any negative gender stereotypes. The creation or propagation of gender stereotypes could lead to issues of discrimination for particular genders, or

worsen other problematic already existing, and potential discrimination. Could the use of the technology help in tackling these stereotypes?

- ○ Yes
- ◉ No

Q9.2. How does it do so?

The question is non related to EO data.

Q9.3. Are there any risks of amplification of gender issues in the use of your technology, or development of your research in the project? Please describe them.

The question is non related to EO data.

Q10.1.
If you consider that an important point has not been asked or you would like to make a comment for feedback, please type it down here.

THANK YOU FOR ANSWERING THE QUESTIONS!

Q1.1. Which type of organisation do you represent in the Project?

- ○ End user
- ◉ Project partner
- ○ Stakeholder

Q1.2. Type-in the name of your organisation or the partner you represent in THEIA project

Institute of Communicaiton and Computer Systems (ICCS)

Q1.3.
Please, type-in your name.

Your name will not be shared with anyone, neither with the other partners of the Consortium, nor published with the survey. It will only be used if internal checking of the results, or feedback is needed by MPLegal.

Q2.1.
Which technology or process is developed or used by your organisation in the project?

- ☐ Data processing pathway
- ☐ Users requirements coordination, demo activities and use-cases
- ☐ Very-High-Resolution Earth Observation tools (Thermal imaging and low-visibility sensing)
- ☐ Very-High-Resolution Earth Observation tools (Data acquisition: Space-based video)
- ☐ Very-High-Resolution Earth Observation tools (Data acquisition: Satellite-Based Multi-Payload Data)
- ☐ Data acquisition: Micro-satellites & Cubesats
- ☐ Data acquisition: UAS-based data
- ☐ Integration of the multi-sensor platform
- ☐ Testing sensors on drones. Drones deployment for testing in real conditions
- ☐ AI for detecting and tracking objects
- ☐ THEIA crowdsourcing tool
- ☐ Database for the Areas of Interest
- ☐ High-velocity transnational data
- ☑ Data fusion & Data models. Data exchange framework

- [ ] Data exchange platform for cloud infrastructure to satellite data
- [ ] National Constellation Data Federation
- [ ] Optimized API Access
- [ ] GeoAI. UAS and terrestrial sensor-based image processing
- [ ] GeoAI. Georeferencing
- [ ] GeoAI. Intelligence Gathering
- [x] GeoAI. Fusion and GeoAI Module
- [ ] THEIA platform
- [ ] Demonstration and validation activities
- [x] Communication, Dissemination, Training and Exploitation
- [ ] Others

Q2.2. If Others, please specify which ones, and within which Work Package in the project.

NA

Q2.3. Briefly describe the objectives and possible benefits of the development and use of the technology in the project.

Within THEIA, ICCS contributes to the development and use of key enabling technologies that enhance Copernicus Security Services: T9.1 develops EO data cubes and harmonised data models to efficiently organise, access, and analyse large multi-temporal datasets, reducing Big Data complexity and enabling scalable AI-driven processing; T10.4 advances multi-source data fusion and GeoAI techniques to integrate EO, SAR, RF, and complementary data into enriched, actionable intelligence products that improve detection accuracy and situational awareness for forced population displacement and security applications; and WP13 ensures that these technological results are effectively communicated, disseminated, and exploited through targeted outreach, training, and stakeholder engagement, maximising visibility, uptake, and long-term impact while supporting EU strategic autonomy and evidence-based decision-making.

Q3.1.
Are you processing or intend to process personal data when developing or using these technologies in THEIA?

Please keep in mind that the terms 'personal data' and 'processing' are rather broad. Processing means the use of personal data at any stage of the Project: collecting, recording, studying and publishing these data, amongst others. Personal data are any information relating to an identified or identifiable natural person. For instance, in THEIA: the processing of a dataset including footage with a camera that records people, the curation of intelligence data from publicly available sources or social media about individuals behaviour, or the collection of information from potential end-users that identify the counterparts, or interaction with them. All these activities imply the processing of personal data, and require an affirmative answer. On the other hand, processing datasets that solely include technical data about UAVs, satellites signal, or geo-spacial resources would not be considered processing of personal data. ***When in doubt, you generally process some personal data. If you have any questions about this, or do not exactly know if you process personal data, please contact MPlegal before continuing with the survey.***

- ( ) Yes
- (•) No

Q3.2.
Please specify the types of personal data which you process.

The categories below are provided for orientation and are not necessarily needed for the purposes of the project. Please specify those relevant to your activities.

This question was not displayed to the respondent.

Q3.3. Develop your previous answer, if it is necessary for any category, or if you clicked "Others".

This question was not displayed to the respondent.

Q3.4.
How will you obtain the personal data?

This question was not displayed to the respondent.

Q3.5. Please specify the sources and means of receiving with regards to all the categories of personal data.

This question was not displayed to the respondent.

Q3.6. Develop and classify per set of personal data the sources.

E.g. Identification data (name and email) are obtained directly from data subjects through a website. Biometric data (facial geometry) are obtained from existing datasets through

This question was not displayed to the respondent.

Q3.7. People need to be informed of the processing of their personal data, unless they are obtained indirecty or anonymised. How do you inform the data subject about the processing activity of personal data?

Please come back to MPlegal with any questions regarding this aspect.

This question was not displayed to the respondent.

Q3.8.
Whose personal data is being processed?

Please describe the data subjects, i.e., the individuals or groups of research participants whose personal data will be collected and processed during the project.

This question was not displayed to the respondent.

Q3.9.
How will you arrange the personal data?

Please describe the datasets of personal data that you have, and map basically your information flows (i.e. what data, where it comes from and where it goes – if it is within your organisation, mention the department; if outside, which partners. **This needs to be a basic answer, which will be developed and used as a base for developing a Data flow map in next deliverables for THEIA.**

This question was not displayed to the respondent.

Q3.10.
What do you want to achieve by collecting the personal data?

Please describe for all the categories of personal data.

This question was not displayed to the respondent.

Q3.11.
How will you use the personal data?

Please describe briefly and precisely for all the categories of personal data.

This question was not displayed to the respondent.

Q3.12.
Is the processing of the personal data really necessary to achieve your purpose?

This question was not displayed to the respondent.

Q3.13. Have you explored alternative means to the use of personal data? (mock data, anonymous dataset, fewer variables of personal data…) How satisfactory would they be to achieve the same outcome?

This question was not displayed to the respondent.

Q3.14.
Where will the personal data be stored?

Please explain the location

This question was not displayed to the respondent.

Q3.15. Where are these servers / storage of personal data?

This question was not displayed to the respondent.

Q3.16.
Will you share the datasets of personal data with third parties, not members of the THEIA consortium?

This question was not displayed to the respondent.

Q3.17.
If yes, please explain the reasons and name the receivers. Please specify if these receivers are located in the European Union or abroad.

This question was not displayed to the respondent.

Q3.18.
Will you cooperate with other partners or external entities for the processing of the personal data?

This question was not displayed to the respondent.

Q3.19.
***If yes**, please specify:*

This question was not displayed to the respondent.

Q3.20.
If you engage with other entities to assist you in data processing, what type of work do they develop? How do you make sure that they comply with data protection principles?
Please describe data types and purposes of joint processing.

This question was not displayed to the respondent.

Q3.21.
Will you work with an external online tool, or other cloud computing solution to process personal data?
If so, which one? Do you know the geographical location for storage of information of such tool or cloud servers (e.g. Europe, US, Canada, Japan)?

This question was not displayed to the respondent.

Q3.22.
In your view, do you think you will need to store the personal data collected for this project after its ending?

Could you please provide a justification, in the light of the purpose for which you process personal data?

This question was not displayed to the respondent.

Q3.23.
Would you be willing to anonymise the data?

Data anonymisation *is a process applied to personal data after which it is no longer possible, now, or in the future, to trace the identity of the individual. It is normally done by separating the elements in the dataset that allow identification. Or assigning random codes of identification to the datasets that cannot be traced back to the original data subject, through encryption.*

This question was not displayed to the respondent.

Q3.24.
***If no**, please provide the reasons.*

This question was not displayed to the respondent.

Q3.25.
Would you be willing to pseudonymise the data?

Pseudonymisation *is a process applied to personal data, replacing the identifiable parts of the dataset with a code or reference number, using an agreed upon code. If you need it, you can reverse the process, and obtain back the individual identity through the used code.*

This question was not displayed to the respondent.

Q3.26.
***If no**, please provide the reasons.*

This question was not displayed to the respondent.

Q3.27. Will you implement data protection by design and by default measures?

Some examples of these measures are providing the control to the data subject over his/her personal data once the technology is implemented. Or reduce the data needed and pseudonymise it.

This question was not displayed to the respondent.

Q3.28.
If yes, develop which ones**. If not**, please provide the reasons.

This question was not displayed to the respondent.

Q3.29.
Will your technology be used for profiling data subjects and/or take automated decisions based solely on the processing of personal data from the data subject? This includes, amongst others, feeding Artificial Intelligence models with the data, in order to obtain decisions over these data subjects.

This question was not displayed to the respondent.

Q3.30. If so, what kind of decisions?

This question was not displayed to the respondent.

Q3.31.
Do you follow or comply with any code of conduct or certification scheme in connection to the processing of personal data? For instance, ISO/IEC 27001:2022 standard for Information security, cybersecurity and privacy protection, Information security management systems; ISO/IEC 42005 Information technology — Artificial intelligence (AI) — AI system impact assessment, or the International Association of Privacy Professionals (IAPP) certifications.

This question was not displayed to the respondent.

Q3.32.
Please identify and provide, if possible, the document or link to the document of certification.

This question was not displayed to the respondent.

Q3.33.
What will be the measures that you will take to secure the personal data that you process?

This question was not displayed to the respondent.

Q3.34.
Data subjects have certain rights under European law regarding the use and processing of their personal data. Do you already have a structure to ensure that data subjects are able to exercise their data subjects rights?

Some examples of these are the right of access to their personal data collected for the purposes of the project, right to erasure such data, right to rectification, right to data portability, possibility for the data subject to withdraw consent. The canalisations of those requests through a Data Protection Officer could be an example of an existing structure.

This question was not displayed to the respondent.

Q3.35.
Please specify technical (e.g. specific email address for requests, software or in-built secure system allowing data subjects to access their own personal data in a transparent way) and organisational measures (e.g. who will provide the information to the data subject) to secure the personal data that you already put in place?

Will you need to limit those data subject rights? If so, please specify which one(s) and the reason to do so.

This question was not displayed to the respondent.

Q3.36. How large is the volume of personal data that you process in the project?

This question was not displayed to the respondent.

Q3.37. Do you process any personal data of children?

Meaning underage people, below the age of 16 years old.

This question was not displayed to the respondent.

Q3.38. Where do you obtain the personal data from children?

i.e. directly from them, from existing datasets, from their parents.

This question was not displayed to the respondent.

Q3.39. If you process personal data from minors, do you contact their parents/legal guardians? What information do you share with them about the data processing?

This question was not displayed to the respondent.

Q3.40. Are third parties involved in the processing of personal data?

This question was not displayed to the respondent.

Q3.41. Who are these third parties? What do they do with the personal data?

This question was not displayed to the respondent.

Q3.42. Please, justify your answer. For instance: we do not process personal data, because all the information that we use in the research project is technical data. Another cause will be that you access personal information, but you cannot identify individuals (anonymisation of personal data). Provide as many details as possible, and examples of the information.

We do not process personal data, because all the information that we use in the research project is technical data. The technologies developed and used in the project rely exclusively on technical, geospatial, and aggregated information, primarily derived from Earth Observation (EO) data, such as satellite imagery (EO, SAR), Radio Frequency (RF) measurements, and other non-space datasets. These data sources capture physical, environmental, and infrastructural characteristics (e.g., land cover changes, movement patterns at area level, infrastructure density) and do not contain names, identifiers, biometric data, or any information linked to identifiable natural persons.

Q4.1. Do you use existing datasets in your research in the project?

- (●) Yes
- ( ) No

Q4.2. What is the origin of the datasets?

- ( ) They were in our possesion before the start of the project.
- (●) They are publicly available.
- ( ) We obtained them after the start of the project free of cost.
- ( ) We obtained them after the start of the project with a licensing access commercial agreement.
- ( ) I do not know.

Q4.3. Do you consider that the datasets may include personal data in them? Please refer to the information in the previous questions from section 2 about personal data.

- ( ) Definitely yes. It is possible to identify individuals within the dataset.
- ( ) Definitely yes. The data are anonymised. There is personal information in the dataset, but it is not possible to identify the individual.
- ( ) Probably yes.
- (●) Probably no.
- ( ) Definitely no.

Q5.1.
Do you think the use or development of the technology might impact privacy of individuals? (such as migrants, including displaced population due to armed conflicts or climate change, minors, undocumented people, and refugees)

Please keep in mind that privacy might be affected without processing of personal data (for example, drones flying above a private house, satellites capturing metrics of properties and terrain). **If you have any questions about this, or do not exactly know if privacy may be impacted, please contact MPlegal before continuing with the survey.**

- ◯ Yes
- ◉ No
- ◯ Maybe

Q5.2. How does your use or development of the technology potentially impact privacy of individuals?

This question was not displayed to the respondent.

Q5.3.
Is this impact on privacy adequate and necessary to achieve the purpose for the development of this technology? For instance, develop the mission and mandate of a public entity, or provide a technical-tool/research that cannot be developed in any other way.

This question was not displayed to the respondent.

Q5.4. Please explain why.

This question was not displayed to the respondent.

Q5.5.
Are there less invasive solutions that can be used to achieve the same purpose effectively?

This question was not displayed to the respondent.

Q5.6. If yes, which are they, and why are they not used?

This question was not displayed to the respondent.

Q5.7. Do you think the benefits which result from the ‘adequate and necessary’ (research) activity are higher than the impact that it will cause for the privacy of the user?

This question was not displayed to the respondent.

Q5.8. Please explain why.

This question was not displayed to the respondent.

Q5.9. Does the implementation or use of the technology affect the subjects moral, religious or cultural integrity?

This question was not displayed to the respondent.

Q6.1.
What would be, in your opinion, the benefit for the end-users of the technology and society?

In my opinion, the technology developed in THEIA offers significant benefits both for end-users and for society at large by transforming complex, fragmented data into timely, reliable, and actionable intelligence. For end-users, such as EU agencies, national authorities, and crisis-management bodies, the main benefit lies in improved situational awareness and decision-making. By combining Earth Observation data with advanced data cubes, multi-source data fusion, and GeoAI analytics, the technology enables earlier detection of emerging population displacement patterns, more accurate assessments of evolving crises, and better coordination of responses. This reduces uncertainty, supports evidence-based planning, and allows resources to be deployed more efficiently and responsibly. For society, the technology contributes to enhanced security, resilience, and humanitarian response while fully respecting fundamental rights. By relying on aggregated, anonymised, and non-intrusive data, it helps authorities understand large-scale dynamics without targeting individuals.

Q6.2.
Are there possible safety risks for the subjects related to the use of the technology?

- ○ Yes
- ○ No
- ◉ There might be.

Q6.3. Please, describe them, or justify the negative answer. For instance: there are risks, but we foresee safeguards that reduce them.

The use of the technology in THEIA may involve indirect safety risks, mainly related to the potential misuse or misinterpretation of analytical outputs rather than to direct impacts on individuals, as the project does not process personal or identifiable data. Such risks could include over-reliance on AI-generated results, inference of sensitive patterns at group or area level, or unauthorized access to operational information, which could negatively affect vulnerable populations if used outside the intended scope. These risks are mitigated through strict purpose limitation, role-based access control, secure data processing environments, and the delivery of results at appropriate levels of spatial and temporal aggregation. In addition, all AI-based outputs are designed to support, not replace, human decision-making, ensuring a human-in-the-loop approach, transparency of analytical confidence, and compliance with EU ethical principles and fundamental rights.

Q6.4.
What technical and organizational measures can be taken to ensure and increase safety of the technology for end-users and data subjects?

The safety of the technology in THEIA can be ensured and enhanced through a combination of robust technical and organizational measures, including secure system architectures with encryption of data at rest and in transit, strong authentication and role-based access control to limit access to sensitive outputs, and systematic data minimisation and aggregation to prevent inference of information about individuals or small groups. AI and data-fusion components are designed as decision-support tools with human-in-the-loop validation, transparency features, and confidence indicators to reduce automation bias and misinterpretation. At the organizational level, clear governance and acceptable-use policies, defined roles and responsibilities, regular risk assessments, and security audits are implemented, alongside user training and awareness activities. These measures, combined with compliance with GDPR, EU ethics requirements, and fundamental-rights principles, ensure that the technology is used responsibly, securely, and safely for both end-users and affected populations.

Q6.5. Are there any technical and organizational measures which could be taken to increase trust of the society and individuals in the use of the technology?

Trust in the use of the technology can be strengthened through a combination of transparent technical design and robust organizational practices, including the clear documentation and communication of data sources, processing methods, and limitations of AI-based analytics, as well as the use of explainable and auditable AI models that provide traceability and confidence indicators. Technical measures such as data minimisation, aggregation, secure processing environments, and strict access controls help demonstrate responsible handling of information, while organizational measures, including clear governance frameworks, ethical guidelines, human oversight, and regular risk and compliance reviews, ensure accountability and proper use. In addition, proactive communication and dissemination activities that explain the purpose, benefits, and safeguards of the technology to stakeholders and the public, combined with training for end-users, help foster transparency, understanding, and long-term societal trust.

Q6.6.
Do you foresee any ethical issues related to the development or use of the technology?

- (●) Yes
- ( ) No

Q6.7. Please describe them.

The development and use of the technology may raise ethical issues primarily related to governance, accountability, and potential misuse rather than direct impacts on individuals, as the system does not process identifiable personal data. Risks include mission creep beyond the intended crisis-management scope, indirect impacts on fundamental rights if outputs are used to support restrictive or discriminatory measures, and biases arising from uneven data coverage or limitations in AI models. There is also a risk of over-reliance on automated analyses, which could reduce human accountability, as well as the possibility of sensitive inferences about vulnerable groups if high-resolution or fused datasets are shared without adequate safeguards. These ethical concerns can be mitigated through clear purpose limitation, human-in-the-loop decision-making, transparency and explainability of AI outputs, strict access controls, data aggregation, and continuous ethical oversight aligned with EU values and fundamental-rights principles.

Q7.1. Are the data used in the project susceptible of misuse? Could they be used, once processed, in a harmful way for the Project or for society?

While the data used in THEIA are primarily technical, geospatial, and non-personal in nature, and are collected and processed for clearly defined research and operational purposes, it is acknowledged that, as with any advanced analytical technology, there is a theoretical potential for misuse if outputs were to be interpreted or applied outside their intended context. In particular, highly processed or aggregated geospatial insights could be misunderstood or taken out of context, potentially leading to unintended or sub-optimal decisions. However, within THEIA, this risk is carefully addressed through strict purpose limitation, controlled access, appropriate aggregation of results, and a human-in-the-loop approach that ensures expert interpretation. As a result, the data and derived products are designed to support responsible, ethical, and evidence-based decision-making, with safeguards in place to prevent harmful use for the project or for society.

Q7.2. Are there any measures already implemented which would prevent this misuse to happen?

- (●) Yes
- ( ) No

Q7.3. Detail them or suggest new ones that could be implemented.

Within THEIA, misuse is already mitigated through purpose limitation, controlled access to data and derived products via authentication and role-based authorisation on a need-to-know basis, and “data minimisation by design,” where outputs are shared at appropriate spatial/temporal aggregation levels to avoid sensitive inference about vulnerable groups. The platform and workflows can further protect against misinterpretation through human-in-the-loop validation, analyst review gates before operational dissemination, and the inclusion of confidence/uncertainty indicators and provenance metadata so end-users understand limitations and context.

Q8.1.
Are there any risks of stigmatisation or discrimination, to your knowledge, in the use of these technologies in GeoAI and law enforcement?

The use of data for law enforcement is a sensitive domain for the general public. Particularly, border surveillance and security raises many societal and ethical questions. The treatment at large scale of information about borders and personal data about migrants needs to be performed in a comprehensive, sensible and protected way. Security measures and responses must be tailored to consider the needs and of vulnerable groups. The potential risk of misinformation must also be considered, as well as the potential generation or amplification of harmful stereotypes concerning these vulnerable groups.

- (●) Yes
- ( ) No

Q8.2. Are there any direct risks of misinformation associated to the use of these technologies?

- (●) Yes
- ( ) No

Q8.3. If any of these risks is spotted, what is the procedure you would follow to minimise and correct the affected stigmatisation or discrimination?

If any risk of stigmatisation, discrimination, or misinformation is identified, the project would immediately initiate a mitigation procedure that includes suspending or restricting the use or dissemination of the affected outputs, conducting an expert review to assess the source of the issue (data, model, interpretation, or communication), and correcting or withdrawing the results where necessary. The issue would be documented and addressed through adjustments to data processing, aggregation levels, model parameters, or user guidance, while reinforcing human-in-the-loop validation and contextual explanations. Where relevant, communication materials would be updated to avoid stigmatising language, and end-users would be informed and trained to ensure responsible interpretation and use, in line with ethical principles, fundamental-rights safeguards, and project governance rules.

Q9.1. THEIA project has endeavoured to develop the research with attention to gender, inclusion, and adequate social norms. This requires not to consider, and not to inflict any negative gender stereotypes. The creation or propagation of gender stereotypes could lead to issues of discrimination for particular genders, or worsen other problematic already existing, and potential discrimination. Could the use of the technology help in tackling these stereotypes?

- (●) Yes
- ( ) No

Q9.2. How does it do so?

If designed and communicated carefully, the technology can support tackling gender stereotypes rather than reinforcing them. Because THEIA's outputs are based on aggregated, non-identifying geospatial indicators (e.g., area-level trends, infrastructure pressure, environmental conditions, accessibility of services) rather than profiling individuals, it can help shift narratives away from assumptions about "who migrants are" and toward evidence-based understanding of needs and risks. It can also support more inclusive decision-making by enabling gender-sensitive planning at the operational level (e.g., resource allocation, protection measures, and safe infrastructure placement) based on objective indicators rather than stereotypes. To ensure it genuinely helps tackle stereotypes, the project should pair the technology with inclusive governance and communication safeguards: avoid gendered or stigmatising labels in dashboards and reports, validate interpretations with relevant stakeholders and experts, apply fairness and bias checks where any demographic proxy is involved, and frame outputs in terms of rights, protection, and needs. When used this way, THEIA can contribute to more responsible narratives and more equitable responses—supporting inclusion and reducing the space for stereotypical assumptions.

Q9.3. Are there any risks of amplification of gender issues in the use of your technology, or development of your research in the project? Please describe them.

While THEIA is designed to avoid individual profiling and to work with aggregated, non-identifying geospatial intelligence, there are still potential risks of unintentionally amplifying gender issues if outputs are interpreted or communicated without sufficient context. For example, stakeholders could draw gendered assumptions from "hotspot" maps or trend indicators, or use simplified narratives that associate displacement dynamics with stereotypes about particular genders. If any ancillary datasets or expert inputs include biased assumptions, or if communication materials use insensitive wording or imagery, this could reinforce existing inequalities. There is also a risk that operational decisions based on area-level insights could overlook gender-differentiated needs unless explicitly considered, leading to unequal outcomes in planning or resource allocation. These risks are mitigated through careful framing of outputs as decision-support, inclusive review of communication, human-in-the-loop validation, and ensuring that gender and inclusion considerations are systematically embedded in analysis and stakeholder engagement.

Q10.1.
If you consider that an important point has not been asked or you would like to make a comment for feedback, please type it down here.

THANK YOU FOR ANSWERING THE QUESTIONS!

Q1.1. Which type of organisation do you represent in the Project?

- ○ End user
- ◉ Project partner
- ○ Stakeholder

Q1.2. Type-in the name of your organisation or the partner you represent in THEIA project

SPACE-SI

Q1.3.
Please, type-in your name.

Your name will not be shared with anyone, neither with the other partners of the Consortium, nor published with the survey. It will only be used if internal checking of the results, or feedback is needed by MPLegal.

Q2.1.
Which technology or process is developed or used by your organisation in the project?

- ☐ Data processing pathway
- ☐ Users requirements coordination, demo activities and use-cases
- ☐ Very-High-Resolution Earth Observation tools (Thermal imaging and low-visibility sensing)
- ☑ Very-High-Resolution Earth Observation tools (Data acquisition: Space-based video)
- ☑ Very-High-Resolution Earth Observation tools (Data acquisition: Satellite-Based Multi-Payload Data)
- ☑ Data acquisition: Micro-satellites & Cubesats
- ☐ Data acquisition: UAS-based data
- ☐ Integration of the multi-sensor platform
- ☐ Testing sensors on drones. Drones deployment for testing in real conditions
- ☐ AI for detecting and tracking objects
- ☐ THEIA crowdsourcing tool
- ☐ Database for the Areas of Interest
- ☐ High-velocity transnational data
- ☐ Data fusion & Data models. Data exchange framework

- [ ] Data exchange platform for cloud infrastructure to satellite data
- [ ] National Constellation Data Federation
- [ ] Optimized API Access
- [ ] GeoAI. UAS and terrestrial sensor-based image processing
- [ ] GeoAI. Georeferencing
- [ ] GeoAI. Intelligence Gathering
- [ ] GeoAI. Fusion and GeoAI Module
- [ ] THEIA platform
- [x] Demonstration and validation activities
- [ ] Communication, Dissemination, Training and Exploitation
- [ ] Others

Q2.2. If Others, please specify which ones, and within which Work Package in the project.

Q2.3. Briefly describe the objectives and possible benefits of the development and use of the technology in the project.

Advantages of space-based video are imroved and faster object recognition, potential for 3D modelling (different observation angles), mitigate effects of cloud coverage, movement identification and analysis.

Q3.1.
Are you processing or intend to process personal data when developing or using these technologies in THEIA?

Please keep in mind that the terms 'personal data' and 'processing' are rather broad. Processing means the use of personal data at any stage of the Project: collecting, recording, studying and publishing these data, amongst others. Personal data are any information relating to an identified or identifiable natural person. For instance, in THEIA: the processing of a dataset including footage with a camera that records people, the curation of intelligence data from publicly available sources or social media about individuals behaviour, or the collection of information from potential end-users that identify the counterparts, or interaction with them. All these activities imply the processing of personal data, and require an affirmative answer. On the other hand, processing datasets that solely include technical data about UAVs, satellites signal, or geo-spacial resources would not be considered processing of personal data. ***When in doubt, you generally process some personal data. If you have any questions about this, or do not exactly know if you process personal data, please contact MPlegal before continuing with the survey.***

- ( ) Yes
- (•) No

Q3.2.
Please specify the types of personal data which you process.

The categories below are provided for orientation and are not necessarily needed for the purposes of the project. Please specify those relevant to your activities.

This question was not displayed to the respondent.

Q3.3. Develop your previous answer, if it is necessary for any category, or if you clicked "Others".

This question was not displayed to the respondent.

Q3.4.
How will you obtain the personal data?

This question was not displayed to the respondent.

Q3.5. Please specify the sources and means of receiving with regards to all the categories of personal data.

This question was not displayed to the respondent.

Q3.6. Develop and classify per set of personal data the sources.

E.g. Identification data (name and email) are obtained directly from data subjects through a website. Biometric data (facial geometry) are obtained from existing datasets through

This question was not displayed to the respondent.

Q3.7. People need to be informed of the processing of their personal data, unless they are obtained indirecty or anonymised. How do you inform the data subject about the processing activity of personal data?

Please come back to MPlegal with any questions regarding this aspect.

This question was not displayed to the respondent.

Q3.8.
Whose personal data is being processed?

Please describe the data subjects, i.e., the individuals or groups of research participants whose personal data will be collected and processed during the project.

This question was not displayed to the respondent.

Q3.9.
How will you arrange the personal data?

Please describe the datasets of personal data that you have, and map basically your information flows (i.e. what data, where it comes from and where it goes – if it is within your organisation, mention the department; if outside, which partners. **This needs to be a basic answer, which will be developed and used as a base for developing a Data flow map in next deliverables for THEIA.**

This question was not displayed to the respondent.

Q3.10.

What do you want to achieve by collecting the personal data?

Please describe for all the categories of personal data.

This question was not displayed to the respondent.

Q3.11.
How will you use the personal data?

Please describe briefly and precisely for all the categories of personal data.

This question was not displayed to the respondent.

Q3.12.
Is the processing of the personal data really necessary to achieve your purpose?

This question was not displayed to the respondent.

Q3.13. Have you explored alternative means to the use of personal data? (mock data, anonymous dataset, fewer variables of personal data…) How satisfactory would they be to achieve the same outcome?

This question was not displayed to the respondent.

Q3.14.
Where will the personal data be stored?

Please explain the location

This question was not displayed to the respondent.

Q3.15. Where are these servers / storage of personal data?

This question was not displayed to the respondent.

Q3.16.
Will you share the datasets of personal data with third parties, not members of the THEIA consortium?

This question was not displayed to the respondent.

Q3.17.
If yes, please explain the reasons and name the receivers. Please specify if these receivers are located in the European Union or abroad.

This question was not displayed to the respondent.

Q3.18.
Will you cooperate with other partners or external entities for the processing of the personal data?

This question was not displayed to the respondent.

Q3.19.
***If yes**, please specify:*

This question was not displayed to the respondent.

Q3.20.
If you engage with other entities to assist you in data processing, what type of work do they develop? How do you make sure that they comply with data protection principles?
Please describe data types and purposes of joint processing.

This question was not displayed to the respondent.

Q3.21.
Will you work with an external online tool, or other cloud computing solution to process personal data?
If so, which one? Do you know the geographical location for storage of information of such tool or cloud servers (e.g. Europe, US, Canada, Japan)?

This question was not displayed to the respondent.

Q3.22.
In your view, do you think you will need to store the personal data collected for this project after its ending?

Could you please provide a justification, in the light of the purpose for which you process personal data?

This question was not displayed to the respondent.

Q3.23.
Would you be willing to anonymise the data?

Data anonymisation *is a process applied to personal data after which it is no longer possible, now, or in the future, to trace the identity of the individual. It is normally done by separating the elements in the dataset that allow identification. Or assigning random codes of identification to the datasets that cannot be traced back to the original data subject, through encryption.*

This question was not displayed to the respondent.

Q3.24.
***If no**, please provide the reasons.*

This question was not displayed to the respondent.

Q3.25.
Would you be willing to pseudonymise the data?

Pseudonymisation *is a process applied to personal data, replacing the identifiable parts of the dataset with a code or reference number, using an agreed upon code. If you need it, you can reverse the process, and obtain back the individual identity through the used code.*

This question was not displayed to the respondent.

Q3.26.
***If no**, please provide the reasons.*

This question was not displayed to the respondent.

Q3.27. Will you implement data protection by design and by default measures?

Some examples of these measures are providing the control to the data subject over his/her personal data once the technology is implemented. Or reduce the data needed and pseudonymise it.

This question was not displayed to the respondent.

Q3.28.
If yes, develop which ones**. If not**, please provide the reasons.

This question was not displayed to the respondent.

Q3.29.
Will your technology be used for profiling data subjects and/or take automated decisions based solely on the processing of personal data from the data subject? This includes, amongst others, feeding Artificial Intelligence models with the data, in order to obtain decisions over these data subjects.

This question was not displayed to the respondent.

Q3.30. If so, what kind of decisions?

This question was not displayed to the respondent.

Q3.31.
Do you follow or comply with any code of conduct or certification scheme in connection to the processing of personal data? For instance, ISO/IEC 27001:2022 standard for Information security, cybersecurity and privacy protection, Information security management systems; ISO/IEC 42005 Information technology — Artificial intelligence (AI) — AI system impact assessment, or the International Association of Privacy Professionals (IAPP) certifications.

This question was not displayed to the respondent.

Q3.32.
Please identify and provide, if possible, the document or link to the document of certification.

This question was not displayed to the respondent.

Q3.33.
What will be the measures that you will take to secure the personal data that you process?

This question was not displayed to the respondent.

Q3.34.

Data subjects have certain rights under European law regarding the use and processing of their personal data. Do you already have a structure to ensure that data subjects are able to exercise their data subjects rights?

Some examples of these are the right of access to their personal data collected for the purposes of the project, right to erasure such data, right to rectification, right to data portability, possibility for the data subject to withdraw consent. The canalisations of those requests through a Data Protection Officer could be an example of an existing structure.

This question was not displayed to the respondent.

Q3.35.
Please specify technical (e.g. specific email address for requests, software or in-built secure system allowing data subjects to access their own personal data in a transparent way) and organisational measures (e.g. who will provide the information to the data subject) to secure the personal data that you already put in place?

Will you need to limit those data subject rights? If so, please specify which one(s) and the reason to do so.

This question was not displayed to the respondent.

Q3.36. How large is the volume of personal data that you process in the project?

This question was not displayed to the respondent.

Q3.37. Do you process any personal data of children?

Meaning underage people, below the age of 16 years old.

This question was not displayed to the respondent.

Q3.38. Where do you obtain the personal data from children?

i.e. directly from them, from existing datasets, from their parents.

This question was not displayed to the respondent.

Q3.39. If you process personal data from minors, do you contact their parents/legal guardians? What information do you share with them about the data processing?

This question was not displayed to the respondent.

Q3.40. Are third parties involved in the processing of personal data?

This question was not displayed to the respondent.

Q3.41. Who are these third parties? What do they do with the personal data?

This question was not displayed to the respondent.

Q3.42. Please, justify your answer. For instance: we do not process personal data, because all the information that we use in the research project is technical data. Another cause will be that you access personal information, but you cannot identify individuals (anonymisation of personal data). Provide as many details as possible, and examples of the information.

We do not process personal data, because all the information that we use in the research project is technical data. Space-based video resolution is 2.8 m so no individual can be recognized id identified.

Q4.1. Do you use existing datasets in your research in the project?

- (●) Yes
- ( ) No

Q4.2. What is the origin of the datasets?

- (●) They were in our possesion before the start of the project.
- ( ) They are publicly available.
- ( ) We obtained them after the start of the project free of cost.
- ( ) We obtained them after the start of the project with a licensing access commercial agreement.
- ( ) I do not know.

Q4.3. Do you consider that the datasets may include personal data in them? Please refer to the information in the previous questions from section 2 about personal data.

- ( ) Definitely yes. It is possible to identify individuals within the dataset.
- ( ) Definitely yes. The data are anonymised. There is personal information in the dataset, but it is not possible to identify the individual.
- ( ) Probably yes.
- ( ) Probably no.
- (●) Definitely no.

Q5.1.
Do you think the use or development of the technology might impact privacy of individuals? (such as migrants, including displaced population due to armed conflicts or climate change, minors, undocumented people, and refugees)

Please keep in mind that privacy might be affected without processing of personal data (for example, drones flying above a private house, satellites capturing metrics of properties and terrain). **If you have any questions about this, or do not exactly know if privacy may be impacted, please contact MPlegal before continuing with the survey.**

- ( ) Yes
- (●) No

◯ Maybe

Q5.2. How does your use or development of the technology potentially impact privacy of individuals?

This question was not displayed to the respondent.

Q5.3.
Is this impact on privacy adequate and necessary to achieve the purpose for the development of this technology? For instance, develop the mission and mandate of a public entity, or provide a technical-tool/research that cannot be developed in any other way.

This question was not displayed to the respondent.

Q5.4. Please explain why.

This question was not displayed to the respondent.

Q5.5.
Are there less invasive solutions that can be used to achieve the same purpose effectively?

This question was not displayed to the respondent.

Q5.6. If yes, which are they, and why are they not used?

This question was not displayed to the respondent.

Q5.7. Do you think the benefits which result from the 'adequate and necessary' (research) activity are higher than the impact that it will cause for the privacy of the user?

This question was not displayed to the respondent.

Q5.8. Please explain why.

This question was not displayed to the respondent.

Q5.9. Does the implementation or use of the technology affect the subjects moral, religious or cultural integrity?

This question was not displayed to the respondent.

Q6.1.
What would be, in your opinion, the benefit for the end-users of the technology and society?

Detection of moving objects.

Q6.2.
Are there possible safety risks for the subjects related to the use of the technology?

- ○ Yes
- ◉ No
- ○ There might be.

Q6.3. Please, describe them, or justify the negative answer. For instance: there are risks, but we foresee safeguards that reduce them.

There is no safety risk for the subjets. Satellite data is taken as remote sensing.

Q6.4.
What technical and organizational measures can be taken to ensure and increase safety of the technology for end-users and data subjects?

There is no safety risk.

Q6.5. Are there any technical and organizational measures which could be taken to increase trust of the society and individuals in the use of the technology?

Remote sensing is already an established, well known and trusted technology.

Q6.6.
Do you foresee any ethical issues related to the development or use of the technology?

- ○ Yes
- ◉ No

Q6.7. Please describe them.

Q7.1. Are the data used in the project susceptible of misuse? Could they be used, once processed, in a harmful way for the Project or for society?

As any Earth observation data of comparable spatial resolution (a lot of it is (freely) available for everyone).

Q7.2. Are there any measures already implemented which would prevent this misuse to happen?

- (●) Yes
- ( ) No

Q7.3. Detail them or suggest new ones that could be implemented.

Data is for internal (project) use only.

Q8.1.
Are there any risks of stigmatisation or discrimination, to your knowledge, in the use of these technologies in GeoAI and law enforcement?

The use of data for law enforcement is a sensitive domain for the general public. Particularly, border surveillance and security raises many societal and ethical questions. The treatment at large scale of information about borders and personal data about migrants needs to be performed in a comprehensive, sensible and protected way. Security measures and responses must be tailored to consider the needs and of vulnerable groups. The potential risk of misinformation must also be considered, as well as the potential generation or amplification of harmful stereotypes concerning these vulnerable groups.

- ( ) Yes
- (●) No

Q8.2. Are there any direct risks of misinformation associated to the use of these technologies?

- ( ) Yes
- (●) No

Q8.3. If any of these risks is spotted, what is the procedure you would follow to minimise and correct the affected stigmatisation or discrimination?

Q9.1. THEIA project has endeavoured to develop the research with attention to gender, inclusion, and adequate social norms. This requires not to consider, and not to inflict any negative gender stereotypes. The creation or propagation of gender stereotypes could lead to issues of discrimination for particular genders, or

worsen other problematic already existing, and potential discrimination. Could the use of the technology help in tackling these stereotypes?

- ○ Yes
- ◉ No

Q9.2. How does it do so?

Q9.3. Are there any risks of amplification of gender issues in the use of your technology, or development of your research in the project? Please describe them.

No.

Q10.1.
If you consider that an important point has not been asked or you would like to make a comment for feedback, please type it down here.

THANK YOU FOR ANSWERING THE QUESTIONS!

Q1.1. Which type of organisation do you represent in the Project?

- ○ End user
- ◉ Project partner
- ○ Stakeholder

Q1.2. Type-in the name of your organisation or the partner you represent in THEIA project

AIT

Q1.3.
Please, type-in your name.

Your name will not be shared with anyone, neither with the other partners of the Consortium, nor published with the survey. It will only be used if internal checking of the results, or feedback is needed by MPLegal.

Q2.1.
Which technology or process is developed or used by your organisation in the project?

- ☐ Data processing pathway
- ☐ Users requirements coordination, demo activities and use-cases
- ☐ Very-High-Resolution Earth Observation tools (Thermal imaging and low-visibility sensing)
- ☐ Very-High-Resolution Earth Observation tools (Data acquisition: Space-based video)
- ☐ Very-High-Resolution Earth Observation tools (Data acquisition: Satellite-Based Multi-Payload Data)
- ☐ Data acquisition: Micro-satellites & Cubesats
- ☐ Data acquisition: UAS-based data
- ☑ Integration of the multi-sensor platform
- ☐ Testing sensors on drones. Drones deployment for testing in real conditions
- ☑ AI for detecting and tracking objects
- ☐ THEIA crowdsourcing tool
- ☐ Database for the Areas of Interest
- ☐ High-velocity transnational data
- ☐ Data fusion & Data models. Data exchange framework

- [ ] Data exchange platform for cloud infrastructure to satellite data
- [ ] National Constellation Data Federation
- [ ] Optimized API Access
- [x] GeoAI. UAS and terrestrial sensor-based image processing
- [ ] GeoAI. Georeferencing
- [ ] GeoAI. Intelligence Gathering
- [ ] GeoAI. Fusion and GeoAI Module
- [ ] THEIA platform
- [ ] Demonstration and validation activities
- [ ] Communication, Dissemination, Training and Exploitation
- [ ] Others

Q2.2. If Others, please specify which ones, and within which Work Package in the project.

Q2.3. Briefly describe the objectives and possible benefits of the development and use of the technology in the project.

Ground-based person/vehicle and vessel detection from multi-sensor platform within outdoor environment during 24/7 operation. Benefits are the mobility of the sensor-platform, the augmentation of the CSS with non-EO data, the robustness of the HW for outdoor operation and the utilization of multiple spectral modalities to allow detection even in low-visibility conditions.

Q3.1.
Are you processing or intend to process personal data when developing or using these technologies in THEIA?

Please keep in mind that the terms 'personal data' and 'processing' are rather broad. Processing means the use of personal data at any stage of the Project: collecting, recording, studying and publishing these data, amongst others. Personal data are any information relating to an identified or identifiable natural person. For instance, in THEIA: the processing of a dataset including footage with a camera that records people, the curation of intelligence data from publicly available sources or social media about individuals behaviour, or the collection of information from potential end-users that identify the counterparts, or interaction with them. All these activities imply the processing of personal data, and require an affirmative answer. On the other hand, processing datasets that solely include technical data about UAVs, satellites signal, or geo-spacial resources would not be considered processing of personal data. ***When in doubt, you generally process some personal data. If you have any questions about this, or do not exactly know if you process personal data, please contact MPlegal before continuing with the survey.***

- (●) Yes
- ( ) No

Q3.2.
Please specify the types of personal data which you process.

The categories below are provided for orientation and are not necessarily needed for the purposes of the project. Please specify those relevant to your activities.

- [ ] a) Identification data (e.g. name, data of birth, age, gender, address, email, phone number)
- [ ] b) Personal features
- [ ] c) Financial data
- [ ] d) Physical, physiological or behavioural characteristics, of a natural person, allowing his/her identification.
- [ ] e) Genetic data
- [ ] f) Biometric data
- [ ] g) Other information regarding health, incl. mental health
- [ ] h) Habits
- [ ] i) Family composition
- [ ] j) Hobbies and interests
- [ ] k) Consumption patterns
- [ ] l) Residence or home address
- [ ] m) Education
- [ ] n) Occupation, employment or professional affiliation
- [ ] o) Social security number or other national identification codes (Passport or ID number)
- [ ] p) Racial or ethnic background
- [ ] q) Philosophical or spiritual orientation
- [ ] r) Information on sexual preferences
- [ ] s) Political orientation or opinion
- [ ] t) Membership of trade union or affiliation
- [ ] u) Other memberships
- [x] v) Video footage of individuals
- [ ] w) Others

Q3.3. Develop your previous answer, if it is necessary for any category, or if you clicked "Others".

Q3.4.
How will you obtain the personal data?

- [x] Directly from data subjects
- [ ] Other partners
- [ ] Other sources
- [ ] I do not know

Q3.5. Please specify the sources and means of receiving with regards to all the categories of personal data.

- [x] Sensors
- [x] Video recordings
- [ ] Software
- [ ] Website
- [ ] Questionnaires
- [ ] Existing datasets
- [ ] Other means
- [ ] I do not know

Q3.6. Develop and classify per set of personal data the sources.

E.g. Identification data (name and email) are obtained directly from data subjects through a website. Biometric data (facial geometry) are obtained from existing datasets through

Video Data is recorded by sensors of the multi-sensor platform (RGB & IR).

Q3.7. People need to be informed of the processing of their personal data, unless they are obtained indirecty or anonymised. How do you inform the data subject about the processing activity of personal data?

Please come back to MPlegal with any questions regarding this aspect.

We employ consent forms to inform the individual persons of the recording of their video data, which the individual persons can accept or reject. If rejected the persons are not recorded.

Q3.8.
Whose personal data is being processed?

Please describe the data subjects, i.e., the individuals or groups of research participants whose personal data will be collected and processed during the project.

Data comes from a few willing participants from our organization.

Q3.9.
How will you arrange the personal data?

Please describe the datasets of personal data that you have, and map basically your information flows (i.e. what data, where it comes from and where it goes – if it is within your organisation, mention the department; if outside, which partners. **This needs to be a basic answer, which will be developed and used as a base for developing a Data flow map in next deliverables for THEIA.**

AIT has recorded a dataset consisting of different videos of persons in a natural environment using AIT's multi-sensor platform. It will remain within AIT except for the annotation of certain videos, which will be done by a different company (Infoscribe), however this annotation process is not part of THEIA.

Q3.10.
What do you want to achieve by collecting the personal data?

Please describe for all the categories of personal data.

Augmentation and diversification of exisiting public open-source datasets, for evaluations and further developments, with scenes from persons within rural areas.

Q3.11.
How will you use the personal data?

Please describe briefly and precisely for all the categories of personal data.

We will use the annotated data for object detection evaluations and/or further algorithmic development

Q3.12.
Is the processing of the personal data really necessary to achieve your purpose?

- (●) Essential
- ( ) Important
- ( ) Accessory
- ( ) Not necessary

Q3.13. Have you explored alternative means to the use of personal data? (mock data, anonymous dataset, fewer variables of personal data…) How satisfactory would they be to achieve the same outcome?

- (●) No, I have not explored them.
- ( ) Yes, I know them. They would not be effective for the purpose.
- ( ) Yes, I know them. They are currently under use.
- ( ) No, we have not explored them. We will incorporate them in the future.

Q3.14.
Where will the personal data be stored?

Please explain the location

- [ ] Locally, in corporate servers, including those accessible remotely via cloud.

- [x] Locally, in corporate devices.
- [ ] Cloud
- [ ] Third parties servers
- [ ] Other

Q3.15. Where are these servers / storage of personal data?

- (•) In a country member of the European Union
- ( ) In a country outside the European Union
- ( ) Unknown

Q3.16.
Will you share the datasets of personal data with third parties, not members of the THEIA consortium?

- (•) Yes
- ( ) No

Q3.17.
If yes, please explain the reasons and name the receivers. Please specify if these receivers are located in the European Union or abroad.

For annotations, but not as a part of the THEIA project and under a contractual agreement regarding the processing of the data. The main location of the company is in France.

Q3.18.
Will you cooperate with other partners or external entities for the processing of the personal data?

- (•) Yes
- ( ) No

Q3.19.
***If yes**, please specify:*

- (•) We need the cooperation as assisting in our processing activities, and for our own purposes.
- ( ) We negotiate and control together the collaboration. We define jointly the purposes of the processing.
- ( ) Other engagement.

Q3.20.
If you engage with other entities to assist you in data processing, what type of work do they develop? How do you make sure that they comply with data protection principles?
Please describe data types and purposes of joint processing.

Annotation company, via a contract the data processing is defined.

Q3.21.
Will you work with an external online tool, or other cloud computing solution to process personal data?
If so, which one? Do you know the geographical location for storage of information of such tool or cloud servers (e.g. Europe, US, Canada, Japan)?

not in use

Q3.22.
In your view, do you think you will need to store the personal data collected for this project after its ending?

Could you please provide a justification, in the light of the purpose for which you process personal data?

Personal data will be stored after the research project for as long as is necessary to demonstrate good scientific practice in accordance with current guidelines.

Q3.23.
Would you be willing to anonymise the data?

Data anonymisation *is a process applied to personal data after which it is no longer possible, now, or in the future, to trace the identity of the individual. It is normally done by separating the elements in the dataset that allow identification. Or assigning random codes of identification to the datasets that cannot be traced back to the original data subject, through encryption.*

- ○ Yes
- ◉ No

Q3.24.
***If no**, please provide the reasons.*

Generally for computer vision tasks, pseudonymisation is rather applied than anonymisation, because otherwise the dataset quality is too heavily impacted for further processing.

Q3.25.
Would you be willing to pseudonymise the data?

Pseudonymisation *is a process applied to personal data, replacing the identifiable parts of the dataset with a code or reference number, using an agreed upon code. If you need it, you can reverse the process, and obtain back the individual identity through the used code.*

- ○ Yes
- ◉ No

Q3.26.
***If no**, please provide the reasons.*

We are looking into methods of pseudonymisation and their applicability, but cannot guarantee implementation (within the project).

Q3.27. Will you implement data protection by design and by default measures?

Some examples of these measures are providing the control to the data subject over his/her personal data once the technology is implemented. Or reduce the data needed and pseudonymise it.

- ◉ Yes
- ○ No

Q3.28.
If yes, develop which ones**. If not**, please provide the reasons.

Consent forms were applied before the recording of video data, participants were informed about their rights to request information about their data, correct data, restrict the processing of their data, revoke consent for processing their data and to have their data transferred if desired. Additionally the data is stored on a local (European) server with access limited only to employees from our organization directly involved with the data processing. If data needs to be processed by a third party (subcontractor), there is a contractual agreement clearly defining the processing of the data.

Q3.29.
Will your technology be used for profiling data subjects and/or take automated decisions based solely on the processing of personal data from the data subject? This includes, amongst others, feeding Artificial Intelligence models with the data, in order to obtain decisions over these data subjects.

- ○ Yes
- ◉ No

Q3.30. If so, what kind of decisions?

no profiling or personalized results will be generated

Q3.31.

Do you follow or comply with any code of conduct or certification scheme in connection to the processing of personal data? For instance, ISO/IEC 27001:2022 standard for Information security, cybersecurity and privacy protection, Information security management systems; ISO/IEC 42005 Information technology — Artificial intelligence (AI) — AI system impact assessment, or the International Association of Privacy Professionals (IAPP) certifications.

- ○ Yes
- ◉ No

Q3.32.
Please identify and provide, if possible, the document or link to the document of certification.

Q3.33.
What will be the measures that you will take to secure the personal data that you process?

Only storing the data locally, restrictive access rules.

Q3.34.
Data subjects have certain rights under European law regarding the use and processing of their personal data. Do you already have a structure to ensure that data subjects are able to exercise their data subjects rights?

Some examples of these are the right of access to their personal data collected for the purposes of the project, right to erasure such data, right to rectification, right to data portability, possibility for the data subject to withdraw consent. The canalisations of those requests through a Data Protection Officer could be an example of an existing structure.

- ◉ Yes
- ○ No

Q3.35.
Please specify technical (e.g. specific email address for requests, software or in-built secure system allowing data subjects to access their own personal data in a transparent way) and organisational measures (e.g. who will provide the information to the data subject) to secure the personal data that you already put in place?

Will you need to limit those data subject rights? If so, please specify which one(s) and the reason to do so.

Email address of the project leader and organizational DPO are provided to the participants for exercising their full rights to their data.

Q3.36. How large is the volume of personal data that you process in the project?

- (●) Small
- ( ) Large
- ( ) Not processing any personal data

Q3.37. Do you process any personal data of children?

Meaning underage people, below the age of 16 years old.

- (●) Definitely not
- ( ) Probably not
- ( ) Probably yes
- ( ) Definitely yes

Q3.38. Where do you obtain the personal data from children?

i.e. directly from them, from existing datasets, from their parents.

Not applicable

Q3.39. If you process personal data from minors, do you contact their parents/legal guardians? What information do you share with them about the data processing?

Not applicable

Q3.40. Are third parties involved in the processing of personal data?

- ( ) No.
- (●) Yes, as contractors, performing some specific tasks under our instructions.
- ( ) Yes, we grant them access to the personal data.
- ( ) Yes, they have the same control over the data that we have.
- ( ) Yes, but we do not know the details.

Q3.41. Who are these third parties? What do they do with the personal data?

Annotation of the data with labels and bounding boxes

Q3.42. Please, justify your answer. For instance: we do not process personal data, because all the information that we use in the research project is technical data. Another cause will be that you access personal information, but you cannot identify individuals (anonymisation of personal data). Provide as many details as possible, and examples of the information.

This question was not displayed to the respondent.

Q4.1. Do you use existing datasets in your research in the project?

- (●) Yes
- ( ) No

Q4.2. What is the origin of the datasets?

- ( ) They were in our possesion before the start of the project.
- (●) They are publicly available.
- ( ) We obtained them after the start of the project free of cost.
- ( ) We obtained them after the start of the project with a licensing access commercial agreement.
- ( ) I do not know.

Q4.3. Do you consider that the datasets may include personal data in them? Please refer to the information in the previous questions from section 2 about personal data.

- ( ) Definitely yes. It is possible to identify individuals within the dataset.
- ( ) Definitely yes. The data are anonymised. There is personal information in the dataset, but it is not possible to identify the individual.
- (●) Probably yes.
- ( ) Probably no.
- ( ) Definitely no.

Q5.1.
Do you think the use or development of the technology might impact privacy of individuals? (such as migrants, including displaced population due to armed conflicts or climate change, minors, undocumented people, and refugees)

Please keep in mind that privacy might be affected without processing of personal data (for example, drones flying above a private house, satellites capturing metrics of properties and terrain). **If you have any questions about this, or do not exactly know if privacy may be impacted, please contact MPlegal before continuing with the survey.**

- (●) Yes
- ( ) No
- ( ) Maybe

Q5.2. How does your use or development of the technology potentially impact privacy of individuals?

Individuals are visible within the ground-based sensor live streams of the RGB camera. Persons are detected as "person" and detection information is sent to the THEIA platform (this can be seen as anonymized data). Data is not stored on the multi-sensor platform. The live video stream (additionally to the detection information) can be requested by end-users of the THEIA platform.

Q5.3.
Is this impact on privacy adequate and necessary to achieve the purpose for the development of this technology? For instance, develop the mission and mandate of a public entity, or provide a technical-tool/research that cannot be developed in any other way.

- (●) Yes
- ( ) No

Q5.4. Please explain why.

RGB camera by default will show environmental details under good lightning conditions. Persons, vehicles, vessels and other structures / objects on the ground-level and slightly above will be visible in an RGB image.

Q5.5.
Are there less invasive solutions that can be used to achieve the same purpose effectively?

- ( ) Yes
- (●) No

Q5.6. If yes, which are they, and why are they not used?

Q5.7. Do you think the benefits which result from the ‘adequate and necessary’ (research) activity are higher than the impact that it will cause for the privacy of the user?

- (●) Definitely Higher
- ( ) Proportionate
- ( ) Non-proportionate
- ( ) Lower

Q5.8. Please explain why.

Limited risk to the privacy due to limited access to the video stream of the camera.

Q5.9. Does the implementation or use of the technology affect the subjects moral, religious or cultural integrity?

- ○ Yes
- ◉ No

Q6.1.
What would be, in your opinion, the benefit for the end-users of the technology and society?

Increased awareness and possibility to take action/offer aid, monitoring events close to the area of interest by using ground-based mutli-sensor platform close to the area of interest. Works 24/7 in an outdoor environment by combining a RGB and a thermal sensor which complement each other in different environmental conditions.

Q6.2.
Are there possible safety risks for the subjects related to the use of the technology?

- ○ Yes
- ◉ No
- ○ There might be.

Q6.3. Please, describe them, or justify the negative answer. For instance: there are risks, but we foresee safeguards that reduce them.

The multi-sensor platform is only equipped with sensors and is not equipped to harm anyone.

Q6.4.
What technical and organizational measures can be taken to ensure and increase safety of the technology for end-users and data subjects?

Q6.5. Are there any technical and organizational measures which could be taken to increase trust of the society and individuals in the use of the technology?

Q6.6.
Do you foresee any ethical issues related to the development or use of the technology?

- ○ Yes
- ◉ No

Q6.7. Please describe them.

Q7.1. Are the data used in the project susceptible of misuse? Could they be used, once processed, in a harmful way for the Project or for society?

Yes, in principle the data could be susceptible to misuse, as they originate from visual sensing of persons. However, the risk of harmful use is low, provided that there is restricted access and many privacy by design principles incorporated: * No storage of raw RGB video * No retention of identifiable imagery * No biometric identification or recognition

Q7.2. Are there any measures already implemented which would prevent this misuse to happen?

- ◉ Yes
- ○ No

Q7.3. Detail them or suggest new ones that could be implemented.

* No storage of raw RGB video * No retention of identifiable imagery * No biometric identification or recognition

Q8.1.
Are there any risks of stigmatisation or discrimination, to your knowledge, in the use of these technologies in GeoAI and law enforcement?

The use of data for law enforcement is a sensitive domain for the general public. Particularly, border surveillance and security raises many societal and ethical questions. The treatment at large scale of information about borders and personal data about migrants needs to be performed in a comprehensive, sensible and protected way. Security measures and responses must be tailored to consider the needs and of vulnerable groups. The potential risk of misinformation must also be considered, as well as the potential generation or amplification of harmful stereotypes concerning these vulnerable groups.

- ○ Yes

- [x] No

Q8.2. Are there any direct risks of misinformation associated to the use of these technologies?

- [ ] Yes
- [x] No

Q8.3. If any of these risks is spotted, what is the procedure you would follow to minimise and correct the affected stigmatisation or discrimination?

Minimization of risks of stigmatization, misinformation, ethical or societal risks are already performed by adhering to privacy by design principles. If additional risks appear/become apparent, additional measures will be discussed with the Ethics partner of the project.

Q9.1. THEIA project has endeavoured to develop the research with attention to gender, inclusion, and adequate social norms. This requires not to consider, and not to inflict any negative gender stereotypes. The creation or propagation of gender stereotypes could lead to issues of discrimination for particular genders, or worsen other problematic already existing, and potential discrimination. Could the use of the technology help in tackling these stereotypes?

- [ ] Yes
- [x] No

Q9.2. How does it do so?

Q9.3. Are there any risks of amplification of gender issues in the use of your technology, or development of your research in the project? Please describe them.

No, object detection algorithms just identify a "person" and not more specific details about the person

Q10.1.
If you consider that an important point has not been asked or you would like to make a comment for feedback, please type it down here.

THANK YOU FOR ANSWERING THE QUESTIONS!

Q1.1. Which type of organisation do you represent in the Project?

- ○ End user
- ◉ Project partner
- ○ Stakeholder

Q1.2. Type-in the name of your organisation or the partner you represent in THEIA project

AIT

Q1.3.
Please, type-in your name.

Your name will not be shared with anyone, neither with the other partners of the Consortium, nor published with the survey. It will only be used if internal checking of the results, or feedback is needed by MPLegal.

Q2.1.
Which technology or process is developed or used by your organisation in the project?

- ☐ Data processing pathway
- ☐ Users requirements coordination, demo activities and use-cases
- ☐ Very-High-Resolution Earth Observation tools (Thermal imaging and low-visibility sensing)
- ☐ Very-High-Resolution Earth Observation tools (Data acquisition: Space-based video)
- ☐ Very-High-Resolution Earth Observation tools (Data acquisition: Satellite-Based Multi-Payload Data)
- ☐ Data acquisition: Micro-satellites & Cubesats
- ☐ Data acquisition: UAS-based data
- ☑ Integration of the multi-sensor platform
- ☐ Testing sensors on drones. Drones deployment for testing in real conditions
- ☑ AI for detecting and tracking objects
- ☐ THEIA crowdsourcing tool
- ☐ Database for the Areas of Interest
- ☐ High-velocity transnational data
- ☐ Data fusion & Data models. Data exchange framework

- [ ] Data exchange platform for cloud infrastructure to satellite data
- [ ] National Constellation Data Federation
- [ ] Optimized API Access
- [x] GeoAI. UAS and terrestrial sensor-based image processing
- [x] GeoAI. Georeferencing
- [ ] GeoAI. Intelligence Gathering
- [ ] GeoAI. Fusion and GeoAI Module
- [ ] THEIA platform
- [x] Demonstration and validation activities
- [x] Communication, Dissemination, Training and Exploitation
- [ ] Others

Q2.2. If Others, please specify which ones, and within which Work Package in the project.

Q2.3. Briefly describe the objectives and possible benefits of the development and use of the technology in the project.

Ground-based person, vehicle and vessel detection from multi-sensor platform within outdoor environment during 24/7 operation. Benefits are the mobility of the sensor-platform, the augmentation of the CSS with non-space data, the robustness of he HW for outdoor operation and the utilization of multiple spectral modalities to allow detection even in low-visibility conditions.

Q3.1.
Are you processing or intend to process personal data when developing or using these technologies in THEIA?

Please keep in mind that the terms 'personal data' and 'processing' are rather broad. Processing means the use of personal data at any stage of the Project: collecting, recording, studying and publishing these data, amongst others. Personal data are any information relating to an identified or identifiable natural person. For instance, in THEIA: the processing of a dataset including footage with a camera that records people, the curation of intelligence data from publicly available sources or social media about individuals behaviour, or the collection of information from potential end-users that identify the counterparts, or interaction with them. All these activities imply the processing of personal data, and require an affirmative answer. On the other hand, processing datasets that solely include technical data about UAVs, satellites signal, or geo-spacial resources would not be considered processing of personal data. ***When in doubt, you generally process some personal data. If you have any questions about this, or do not exactly know if you process personal data, please contact MPlegal before continuing with the survey.***

- ( ) Yes
- (•) No

Q3.2.
Please specify the types of personal data which you process.

The categories below are provided for orientation and are not necessarily needed for the purposes of the project. Please specify those relevant to your activities.

This question was not displayed to the respondent.

Q3.3. Develop your previous answer, if it is necessary for any category, or if you clicked "Others".

This question was not displayed to the respondent.

Q3.4.
How will you obtain the personal data?

This question was not displayed to the respondent.

Q3.5. Please specify the sources and means of receiving with regards to all the categories of personal data.

This question was not displayed to the respondent.

Q3.6. Develop and classify per set of personal data the sources.

E.g. Identification data (name and email) are obtained directly from data subjects through a website. Biometric data (facial geometry) are obtained from existing datasets through

This question was not displayed to the respondent.

Q3.7. People need to be informed of the processing of their personal data, unless they are obtained indirecty or anonymised. How do you inform the data subject about the processing activity of personal data?

Please come back to MPlegal with any questions regarding this aspect.

This question was not displayed to the respondent.

Q3.8.
Whose personal data is being processed?

Please describe the data subjects, i.e., the individuals or groups of research participants whose personal data will be collected and processed during the project.

This question was not displayed to the respondent.

Q3.9.
How will you arrange the personal data?

Please describe the datasets of personal data that you have, and map basically your information flows (i.e. what data, where it comes from and where it goes – if it is within your organisation, mention the department; if outside, which partners. **This needs to be a basic answer, which will be developed and used as a base for developing a Data flow map in next deliverables for THEIA.**

This question was not displayed to the respondent.

Q3.10.

What do you want to achieve by collecting the personal data?

Please describe for all the categories of personal data.

This question was not displayed to the respondent.

Q3.11.
How will you use the personal data?

Please describe briefly and precisely for all the categories of personal data.

This question was not displayed to the respondent.

Q3.12.
Is the processing of the personal data really necessary to achieve your purpose?

This question was not displayed to the respondent.

Q3.13. Have you explored alternative means to the use of personal data? (mock data, anonymous dataset, fewer variables of personal data…) How satisfactory would they be to achieve the same outcome?

This question was not displayed to the respondent.

Q3.14.
Where will the personal data be stored?

Please explain the location

This question was not displayed to the respondent.

Q3.15. Where are these servers / storage of personal data?

This question was not displayed to the respondent.

Q3.16.
Will you share the datasets of personal data with third parties, not members of the THEIA consortium?

This question was not displayed to the respondent.

Q3.17.
If yes, please explain the reasons and name the receivers. Please specify if these receivers are located in the European Union or abroad.

This question was not displayed to the respondent.

Q3.18.
Will you cooperate with other partners or external entities for the processing of the personal data?

This question was not displayed to the respondent.

Q3.19.
***If yes**, please specify:*

This question was not displayed to the respondent.

Q3.20.
If you engage with other entities to assist you in data processing, what type of work do they develop? How do you make sure that they comply with data protection principles?
Please describe data types and purposes of joint processing.

This question was not displayed to the respondent.

Q3.21.
Will you work with an external online tool, or other cloud computing solution to process personal data?
If so, which one? Do you know the geographical location for storage of information of such tool or cloud servers (e.g. Europe, US, Canada, Japan)?

This question was not displayed to the respondent.

Q3.22.
In your view, do you think you will need to store the personal data collected for this project after its ending?

Could you please provide a justification, in the light of the purpose for which you process personal data?

This question was not displayed to the respondent.

Q3.23.
Would you be willing to anonymise the data?

Data anonymisation *is a process applied to personal data after which it is no longer possible, now, or in the future, to trace the identity of the individual. It is normally done by separating the elements in the dataset that allow identification. Or assigning random codes of identification to the datasets that cannot be traced back to the original data subject, through encryption.*

This question was not displayed to the respondent.

Q3.24.
***If no**, please provide the reasons.*

This question was not displayed to the respondent.

Q3.25.
Would you be willing to pseudonymise the data?

Pseudonymisation *is a process applied to personal data, replacing the identifiable parts of the dataset with a code or reference number, using an agreed upon code. If you need it, you can reverse the process, and obtain back the individual identity through the used code.*

This question was not displayed to the respondent.

Q3.26.
***If no**, please provide the reasons.*

This question was not displayed to the respondent.

Q3.27. Will you implement data protection by design and by default measures?

Some examples of these measures are providing the control to the data subject over his/her personal data once the technology is implemented. Or reduce the data needed and pseudonymise it.

This question was not displayed to the respondent.

Q3.28.
If yes, develop which ones**. If not**, please provide the reasons.

This question was not displayed to the respondent.

Q3.29.
Will your technology be used for profiling data subjects and/or take automated decisions based solely on the processing of personal data from the data subject? This includes, amongst others, feeding Artificial Intelligence models with the data, in order to obtain decisions over these data subjects.

This question was not displayed to the respondent.

Q3.30. If so, what kind of decisions?

This question was not displayed to the respondent.

Q3.31.
Do you follow or comply with any code of conduct or certification scheme in connection to the processing of personal data? For instance, ISO/IEC 27001:2022 standard for Information security, cybersecurity and privacy protection, Information security management systems; ISO/IEC 42005 Information technology — Artificial intelligence (AI) — AI system impact assessment, or the International Association of Privacy Professionals (IAPP) certifications.

This question was not displayed to the respondent.

Q3.32.
Please identify and provide, if possible, the document or link to the document of certification.

This question was not displayed to the respondent.

Q3.33.
What will be the measures that you will take to secure the personal data that you process?

This question was not displayed to the respondent.

Q3.34.

Data subjects have certain rights under European law regarding the use and processing of their personal data. Do you already have a structure to ensure that data subjects are able to exercise their data subjects rights?

Some examples of these are the right of access to their personal data collected for the purposes of the project, right to erasure such data, right to rectification, right to data portability, possibility for the data subject to withdraw consent. The canalisations of those requests through a Data Protection Officer could be an example of an existing structure.

This question was not displayed to the respondent.

Q3.35.
Please specify technical (e.g. specific email address for requests, software or in-built secure system allowing data subjects to access their own personal data in a transparent way) and organisational measures (e.g. who will provide the information to the data subject) to secure the personal data that you already put in place?

Will you need to limit those data subject rights? If so, please specify which one(s) and the reason to do so.

This question was not displayed to the respondent.

Q3.36. How large is the volume of personal data that you process in the project?

This question was not displayed to the respondent.

Q3.37. Do you process any personal data of children?

Meaning underage people, below the age of 16 years old.

This question was not displayed to the respondent.

Q3.38. Where do you obtain the personal data from children?

i.e. directly from them, from existing datasets, from their parents.

This question was not displayed to the respondent.

Q3.39. If you process personal data from minors, do you contact their parents/legal guardians? What information do you share with them about the data processing?

This question was not displayed to the respondent.

Q3.40. Are third parties involved in the processing of personal data?

This question was not displayed to the respondent.

Q3.41. Who are these third parties? What do they do with the personal data?

This question was not displayed to the respondent.

Q3.42. Please, justify your answer. For instance: we do not process personal data, because all the information that we use in the research project is technical data. Another cause will be that you access personal information, but you cannot identify individuals (anonymisation of personal data). Provide as many details as possible, and examples of the information.

Within THEIA and the data recording for THEIA either open-source data will be used, or persons recorded with a thermal sensor, that captures the heat signature of the person and no facial features or other distinctive features.

Q4.1. Do you use existing datasets in your research in the project?

- (●) Yes
- ( ) No

Q4.2. What is the origin of the datasets?

- ( ) They were in our possesion before the start of the project.
- (●) They are publicly available.
- ( ) We obtained them after the start of the project free of cost.
- ( ) We obtained them after the start of the project with a licensing access commercial agreement.
- ( ) I do not know.

Q4.3. Do you consider that the datasets may include personal data in them? Please refer to the information in the previous questions from section 2 about personal data.

- ( ) Definitely yes. It is possible to identify individuals within the dataset.
- ( ) Definitely yes. The data are anonymised. There is personal information in the dataset, but it is not possible to identify the individual.
- (●) Probably yes.
- ( ) Probably no.
- ( ) Definitely no.

Q5.1.
Do you think the use or development of the technology might impact privacy of individuals? (such as migrants, including displaced population due to armed conflicts or climate change, minors, undocumented people, and refugees)

Please keep in mind that privacy might be affected without processing of personal data (for example, drones flying above a private house, satellites capturing metrics of properties and terrain). **If you have any questions about this, or do not exactly know if privacy may be impacted, please contact MPlegal before continuing with the survey.**

- ( ) Yes
- (●) No

◯ Maybe

Q5.2. How does your use or development of the technology potentially impact privacy of individuals?

This question was not displayed to the respondent.

Q5.3.
Is this impact on privacy adequate and necessary to achieve the purpose for the development of this technology? For instance, develop the mission and mandate of a public entity, or provide a technical-tool/research that cannot be developed in any other way.

This question was not displayed to the respondent.

Q5.4. Please explain why.

This question was not displayed to the respondent.

Q5.5.
Are there less invasive solutions that can be used to achieve the same purpose effectively?

This question was not displayed to the respondent.

Q5.6. If yes, which are they, and why are they not used?

This question was not displayed to the respondent.

Q5.7. Do you think the benefits which result from the 'adequate and necessary' (research) activity are higher than the impact that it will cause for the privacy of the user?

This question was not displayed to the respondent.

Q5.8. Please explain why.

This question was not displayed to the respondent.

Q5.9. Does the implementation or use of the technology affect the subjects moral, religious or cultural integrity?

This question was not displayed to the respondent.

Q6.1.
What would be, in your opinion, the benefit for the end-users of the technology and society?

Benefits for the end-users are the increased situational awareness provided by THEIA. From AITs side the mobility of the sensor-platform, the augmentation of the CSS with non-space data, the robustness of he HW for outdoor operation and the utilization of multiple spectral modalities to allow detection even in low-visibility conditions are benefits for the end-user. Benefits for society are augmented emergency response systems.

Q6.2.
Are there possible safety risks for the subjects related to the use of the technology?

- ○ Yes
- ◉ No
- ○ There might be.

Q6.3. Please, describe them, or justify the negative answer. For instance: there are risks, but we foresee safeguards that reduce them.

The multi-sensor platform will not have physically harmful effects on anyone, and will not record personal data, thus not violating the personal privacy either.

Q6.4.
What technical and organizational measures can be taken to ensure and increase safety of the technology for end-users and data subjects?

Not applicable

Q6.5. Are there any technical and organizational measures which could be taken to increase trust of the society and individuals in the use of the technology?

Not applicable

Q6.6.
Do you foresee any ethical issues related to the development or use of the technology?

- ○ Yes
- ◉ No

Q6.7. Please describe them.

Not applicable

Q7.1. Are the data used in the project susceptible of misuse? Could they be used, once processed, in a harmful way for the Project or for society?

No

Q7.2. Are there any measures already implemented which would prevent this misuse to happen?

- ○ Yes
- ◉ No

Q7.3. Detail them or suggest new ones that could be implemented.

Not applicable

Q8.1.
Are there any risks of stigmatisation or discrimination, to your knowledge, in the use of these technologies in GeoAI and law enforcement?

The use of data for law enforcement is a sensitive domain for the general public. Particularly, border surveillance and security raises many societal and ethical questions. The treatment at large scale of information about borders and personal data about migrants needs to be performed in a comprehensive, sensible and protected way. Security measures and responses must be tailored to consider the needs and of vulnerable groups. The potential risk of misinformation must also be considered, as well as the potential generation or amplification of harmful stereotypes concerning these vulnerable groups.

- ○ Yes
- ◉ No

Q8.2. Are there any direct risks of misinformation associated to the use of these technologies?

- ○ Yes
- ◉ No

Q8.3. If any of these risks is spotted, what is the procedure you would follow to minimise and correct the affected stigmatisation or discrimination?

Not applicable

Q9.1. THEIA project has endeavoured to develop the research with attention to gender, inclusion, and adequate social norms. This requires not to consider, and not to inflict any negative gender stereotypes. The creation or propagation of gender stereotypes could lead to issues of discrimination for particular genders, or

worsen other problematic already existing, and potential discrimination. Could the use of the technology help in tackling these stereotypes?

- ○ Yes
- ◉ No

Q9.2. How does it do so?

Q9.3. Are there any risks of amplification of gender issues in the use of your technology, or development of your research in the project? Please describe them.

Not applicable

Q10.1.
If you consider that an important point has not been asked or you would like to make a comment for feedback, please type it down here.

THANK YOU FOR ANSWERING THE QUESTIONS!

Q1.1. Which type of organisation do you represent in the Project?

- ○ End user
- ◉ Project partner
- ○ Stakeholder

Q1.2. Type-in the name of your organisation or the partner you represent in THEIA project

ED

Q1.3.
Please, type-in your name.

Your name will not be shared with anyone, neither with the other partners of the Consortium, nor published with the survey. It will only be used if internal checking of the results, or feedback is needed by MPLegal.

Q2.1.
Which technology or process is developed or used by your organisation in the project?

- ☑ Data processing pathway
- ☑ Users requirements coordination, demo activities and use-cases
- ☐ Very-High-Resolution Earth Observation tools (Thermal imaging and low-visibility sensing)
- ☐ Very-High-Resolution Earth Observation tools (Data acquisition: Space-based video)
- ☐ Very-High-Resolution Earth Observation tools (Data acquisition: Satellite-Based Multi-Payload Data)
- ☐ Data acquisition: Micro-satellites & Cubesats
- ☐ Data acquisition: UAS-based data
- ☐ Integration of the multi-sensor platform
- ☐ Testing sensors on drones. Drones deployment for testing in real conditions
- ☐ AI for detecting and tracking objects
- ☐ THEIA crowdsourcing tool
- ☑ Database for the Areas of Interest
- ☐ High-velocity transnational data
- ☐ Data fusion & Data models. Data exchange framework

- [ ] Data exchange platform for cloud infrastructure to satellite data
- [ ] National Constellation Data Federation
- [x] Optimized API Access
- [ ] GeoAI. UAS and terrestrial sensor-based image processing
- [ ] GeoAI. Georeferencing
- [ ] GeoAI. Intelligence Gathering
- [ ] GeoAI. Fusion and GeoAI Module
- [ ] THEIA platform
- [ ] Demonstration and validation activities
- [ ] Communication, Dissemination, Training and Exploitation
- [ ] Others

Q2.2. If Others, please specify which ones, and within which Work Package in the project.

Q2.3. Briefly describe the objectives and possible benefits of the development and use of the technology in the project.

1) Create an index for population displacement based on geospatial data. 2) Georeference Open Source data (collected by other partners)

Q3.1.
Are you processing or intend to process personal data when developing or using these technologies in THEIA?

Please keep in mind that the terms 'personal data' and 'processing' are rather broad. Processing means the use of personal data at any stage of the Project: collecting, recording, studying and publishing these data, amongst others. Personal data are any information relating to an identified or identifiable natural person. For instance, in THEIA: the processing of a dataset including footage with a camera that records people, the curation of intelligence data from publicly available sources or social media about individuals behaviour, or the collection of information from potential end-users that identify the counterparts, or interaction with them. All these activities imply the processing of personal data, and require an affirmative answer. On the other hand, processing datasets that solely include technical data about UAVs, satellites signal, or geo-spacial resources would not be considered processing of personal data. ***When in doubt, you generally process some personal data. If you have any questions about this, or do not exactly know if you process personal data, please contact MPlegal before continuing with the survey.***

- ( ) Yes
- (•) No

Q3.2.
Please specify the types of personal data which you process.

The categories below are provided for orientation and are not necessarily needed for the purposes of the project. Please specify those relevant to your activities.

This question was not displayed to the respondent.

Q3.3. Develop your previous answer, if it is necessary for any category, or if you clicked "Others".

This question was not displayed to the respondent.

Q3.4.
How will you obtain the personal data?

This question was not displayed to the respondent.

Q3.5. Please specify the sources and means of receiving with regards to all the categories of personal data.

This question was not displayed to the respondent.

Q3.6. Develop and classify per set of personal data the sources.

E.g. Identification data (name and email) are obtained directly from data subjects through a website. Biometric data (facial geometry) are obtained from existing datasets through

This question was not displayed to the respondent.

Q3.7. People need to be informed of the processing of their personal data, unless they are obtained indirecty or anonymised. How do you inform the data subject about the processing activity of personal data?

Please come back to MPlegal with any questions regarding this aspect.

This question was not displayed to the respondent.

Q3.8.
Whose personal data is being processed?

Please describe the data subjects, i.e., the individuals or groups of research participants whose personal data will be collected and processed during the project.

This question was not displayed to the respondent.

Q3.9.
How will you arrange the personal data?

Please describe the datasets of personal data that you have, and map basically your information flows (i.e. what data, where it comes from and where it goes – if it is within your organisation, mention the department; if outside, which partners. **This needs to be a basic answer, which will be developed and used as a base for developing a Data flow map in next deliverables for THEIA.**

This question was not displayed to the respondent.

Q3.10.

What do you want to achieve by collecting the personal data?

Please describe for all the categories of personal data.

This question was not displayed to the respondent.

Q3.11.
How will you use the personal data?

Please describe briefly and precisely for all the categories of personal data.

This question was not displayed to the respondent.

Q3.12.
Is the processing of the personal data really necessary to achieve your purpose?

This question was not displayed to the respondent.

Q3.13. Have you explored alternative means to the use of personal data? (mock data, anonymous dataset, fewer variables of personal data…) How satisfactory would they be to achieve the same outcome?

This question was not displayed to the respondent.

Q3.14.
Where will the personal data be stored?

Please explain the location

This question was not displayed to the respondent.

Q3.15. Where are these servers / storage of personal data?

This question was not displayed to the respondent.

Q3.16.
Will you share the datasets of personal data with third parties, not members of the THEIA consortium?

This question was not displayed to the respondent.

Q3.17.
If yes, please explain the reasons and name the receivers. Please specify if these receivers are located in the European Union or abroad.

This question was not displayed to the respondent.

Q3.18.
Will you cooperate with other partners or external entities for the processing of the personal data?

This question was not displayed to the respondent.

Q3.19.
***If yes**, please specify:*

This question was not displayed to the respondent.

Q3.20.
If you engage with other entities to assist you in data processing, what type of work do they develop? How do you make sure that they comply with data protection principles?
Please describe data types and purposes of joint processing.

This question was not displayed to the respondent.

Q3.21.
Will you work with an external online tool, or other cloud computing solution to process personal data?
If so, which one? Do you know the geographical location for storage of information of such tool or cloud servers (e.g. Europe, US, Canada, Japan)?

This question was not displayed to the respondent.

Q3.22.
In your view, do you think you will need to store the personal data collected for this project after its ending?

Could you please provide a justification, in the light of the purpose for which you process personal data?

This question was not displayed to the respondent.

Q3.23.
Would you be willing to anonymise the data?

Data anonymisation *is a process applied to personal data after which it is no longer possible, now, or in the future, to trace the identity of the individual. It is normally done by separating the elements in the dataset that allow identification. Or assigning random codes of identification to the datasets that cannot be traced back to the original data subject, through encryption.*

This question was not displayed to the respondent.

Q3.24.
***If no**, please provide the reasons.*

This question was not displayed to the respondent.

Q3.25.
Would you be willing to pseudonymise the data?

Pseudonymisation *is a process applied to personal data, replacing the identifiable parts of the dataset with a code or reference number, using an agreed upon code. If you need it, you can reverse the process, and obtain back the individual identity through the used code.*

This question was not displayed to the respondent.

Q3.26.
***If no**, please provide the reasons.*

This question was not displayed to the respondent.

Q3.27. Will you implement data protection by design and by default measures?

Some examples of these measures are providing the control to the data subject over his/her personal data once the technology is implemented. Or reduce the data needed and pseudonymise it.

This question was not displayed to the respondent.

Q3.28.
If yes, develop which ones**. If not**, please provide the reasons.

This question was not displayed to the respondent.

Q3.29.
Will your technology be used for profiling data subjects and/or take automated decisions based solely on the processing of personal data from the data subject? This includes, amongst others, feeding Artificial Intelligence models with the data, in order to obtain decisions over these data subjects.

This question was not displayed to the respondent.

Q3.30. If so, what kind of decisions?

This question was not displayed to the respondent.

Q3.31.
Do you follow or comply with any code of conduct or certification scheme in connection to the processing of personal data? For instance, ISO/IEC 27001:2022 standard for Information security, cybersecurity and privacy protection, Information security management systems; ISO/IEC 42005 Information technology — Artificial intelligence (AI) — AI system impact assessment, or the International Association of Privacy Professionals (IAPP) certifications.

This question was not displayed to the respondent.

Q3.32.
Please identify and provide, if possible, the document or link to the document of certification.

This question was not displayed to the respondent.

Q3.33.
What will be the measures that you will take to secure the personal data that you process?

This question was not displayed to the respondent.

Q3.34.

Data subjects have certain rights under European law regarding the use and processing of their personal data. Do you already have a structure to ensure that data subjects are able to exercise their data subjects rights?

Some examples of these are the right of access to their personal data collected for the purposes of the project, right to erasure such data, right to rectification, right to data portability, possibility for the data subject to withdraw consent. The canalisations of those requests through a Data Protection Officer could be an example of an existing structure.

This question was not displayed to the respondent.

Q3.35.
Please specify technical (e.g. specific email address for requests, software or in-built secure system allowing data subjects to access their own personal data in a transparent way) and organisational measures (e.g. who will provide the information to the data subject) to secure the personal data that you already put in place?

Will you need to limit those data subject rights? If so, please specify which one(s) and the reason to do so.

This question was not displayed to the respondent.

Q3.36. How large is the volume of personal data that you process in the project?

This question was not displayed to the respondent.

Q3.37. Do you process any personal data of children?

Meaning underage people, below the age of 16 years old.

This question was not displayed to the respondent.

Q3.38. Where do you obtain the personal data from children?

i.e. directly from them, from existing datasets, from their parents.

This question was not displayed to the respondent.

Q3.39. If you process personal data from minors, do you contact their parents/legal guardians? What information do you share with them about the data processing?

This question was not displayed to the respondent.

Q3.40. Are third parties involved in the processing of personal data?

This question was not displayed to the respondent.

Q3.41. Who are these third parties? What do they do with the personal data?

This question was not displayed to the respondent.

Q3.42. Please, justify your answer. For instance: we do not process personal data, because all the information that we use in the research project is technical data. Another cause will be that you access personal information, but you cannot identify individuals (anonymisation of personal data). Provide as many details as possible, and examples of the information.

We do not access personal information. The information is either publicly available by International Organizations with low granularity or incoming data form partners have no personal information. Thus, we do not process personal data, because all the information that we use in the research project is technical data.

Q4.1. Do you use existing datasets in your research in the project?

- (●) Yes
- ( ) No

Q4.2. What is the origin of the datasets?

- ( ) They were in our possesion before the start of the project.
- (●) They are publicly available.
- ( ) We obtained them after the start of the project free of cost.
- ( ) We obtained them after the start of the project with a licensing access commercial agreement.
- ( ) I do not know.

Q4.3. Do you consider that the datasets may include personal data in them? Please refer to the information in the previous questions from section 2 about personal data.

- ( ) Definitely yes. It is possible to identify individuals within the dataset.
- ( ) Definitely yes. The data are anonymised. There is personal information in the dataset, but it is not possible to identify the individual.
- ( ) Probably yes.
- ( ) Probably no.
- (●) Definitely no.

Q5.1.
Do you think the use or development of the technology might impact privacy of individuals? (such as migrants, including displaced population due to armed conflicts or climate change, minors, undocumented people, and refugees)

Please keep in mind that privacy might be affected without processing of personal data (for example, drones flying above a private house, satellites capturing metrics of properties and terrain). **If you have any questions about this, or do not exactly know if privacy may be impacted, please contact MPlegal before continuing with the survey.**

- ( ) Yes
- (●) No

◯ Maybe

Q5.2. How does your use or development of the technology potentially impact privacy of individuals?

This question was not displayed to the respondent.

Q5.3.
Is this impact on privacy adequate and necessary to achieve the purpose for the development of this technology? For instance, develop the mission and mandate of a public entity, or provide a technical-tool/research that cannot be developed in any other way.

This question was not displayed to the respondent.

Q5.4. Please explain why.

This question was not displayed to the respondent.

Q5.5.
Are there less invasive solutions that can be used to achieve the same purpose effectively?

This question was not displayed to the respondent.

Q5.6. If yes, which are they, and why are they not used?

This question was not displayed to the respondent.

Q5.7. Do you think the benefits which result from the 'adequate and necessary' (research) activity are higher than the impact that it will cause for the privacy of the user?

This question was not displayed to the respondent.

Q5.8. Please explain why.

This question was not displayed to the respondent.

Q5.9. Does the implementation or use of the technology affect the subjects moral, religious or cultural integrity?

This question was not displayed to the respondent.

Q6.1.
What would be, in your opinion, the benefit for the end-users of the technology and society?

Indication of possible population displacement.

Q6.2.
Are there possible safety risks for the subjects related to the use of the technology?

- ○ Yes
- ◉ No
- ○ There might be.

Q6.3. Please, describe them, or justify the negative answer. For instance: there are risks, but we foresee safeguards that reduce them.

n/a

Q6.4.
What technical and organizational measures can be taken to ensure and increase safety of the technology for end-users and data subjects?

n/a

Q6.5. Are there any technical and organizational measures which could be taken to increase trust of the society and individuals in the use of the technology?

n/a

Q6.6.
Do you foresee any ethical issues related to the development or use of the technology?

- ○ Yes
- ◉ No

Q6.7. Please describe them.

n/a

Q7.1. Are the data used in the project susceptible of misuse? Could they be used, once processed, in a harmful way for the Project or for society?

no

Q7.2. Are there any measures already implemented which would prevent this misuse to happen?

- ○ Yes
- ◉ No

Q7.3. Detail them or suggest new ones that could be implemented.

n/a

Q8.1.
Are there any risks of stigmatisation or discrimination, to your knowledge, in the use of these technologies in GeoAI and law enforcement?

The use of data for law enforcement is a sensitive domain for the general public. Particularly, border surveillance and security raises many societal and ethical questions. The treatment at large scale of information about borders and personal data about migrants needs to be performed in a comprehensive, sensible and protected way. Security measures and responses must be tailored to consider the needs and of vulnerable groups. The potential risk of misinformation must also be considered, as well as the potential generation or amplification of harmful stereotypes concerning these vulnerable groups.

- ○ Yes
- ◉ No

Q8.2. Are there any direct risks of misinformation associated to the use of these technologies?

- ○ Yes
- ◉ No

Q8.3. If any of these risks is spotted, what is the procedure you would follow to minimise and correct the affected stigmatisation or discrimination?

The above answers refer to ED's technologies. There are no such issues.

Q9.1. THEIA project has endeavoured to develop the research with attention to gender, inclusion, and adequate social norms. This requires not to consider, and not to inflict any negative gender stereotypes. The creation or propagation of gender stereotypes could lead to issues of discrimination for particular genders, or

worsen other problematic already existing, and potential discrimination. Could the use of the technology help in tackling these stereotypes?

- ○ Yes
- ◉ No

Q9.2. How does it do so?

The techologies provided by ED are gender agnostic.

Q9.3. Are there any risks of amplification of gender issues in the use of your technology, or development of your research in the project? Please describe them.

No

Q10.1.
If you consider that an important point has not been asked or you would like to make a comment for feedback, please type it down here.

THANK YOU FOR ANSWERING THE QUESTIONS!

The answers refer to ED's technology and not the entire THEIA project.

Q1.1. Which type of organisation do you represent in the Project?

- ○ End user
- ◉ Project partner
- ○ Stakeholder

Q1.2. Type-in the name of your organisation or the partner you represent in THEIA project

Creotech Instruments S.A.

Q1.3.
Please, type-in your name.

Your name will not be shared with anyone, neither with the other partners of the Consortium, nor published with the survey. It will only be used if internal checking of the results, or feedback is needed by MPLegal.

Q2.1.
Which technology or process is developed or used by your organisation in the project?

- ☐ Data processing pathway
- ☐ Users requirements coordination, demo activities and use-cases
- ☐ Very-High-Resolution Earth Observation tools (Thermal imaging and low-visibility sensing)
- ☐ Very-High-Resolution Earth Observation tools (Data acquisition: Space-based video)
- ☐ Very-High-Resolution Earth Observation tools (Data acquisition: Satellite-Based Multi-Payload Data)
- ☐ Data acquisition: Micro-satellites & Cubesats
- ☐ Data acquisition: UAS-based data
- ☐ Integration of the multi-sensor platform
- ☐ Testing sensors on drones. Drones deployment for testing in real conditions
- ☐ AI for detecting and tracking objects
- ☐ THEIA crowdsourcing tool
- ☐ Database for the Areas of Interest
- ☐ High-velocity transnational data
- ☑ Data fusion & Data models. Data exchange framework

- [x] Data exchange platform for cloud infrastructure to satellite data
- [x] National Constellation Data Federation
- [x] Optimized API Access
- [ ] GeoAI. UAS and terrestrial sensor-based image processing
- [ ] GeoAI. Georeferencing
- [ ] GeoAI. Intelligence Gathering
- [ ] GeoAI. Fusion and GeoAI Module
- [ ] THEIA platform
- [ ] Demonstration and validation activities
- [ ] Communication, Dissemination, Training and Exploitation
- [ ] Others

Q2.2. If Others, please specify which ones, and within which Work Package in the project.

Q2.3. Briefly describe the objectives and possible benefits of the development and use of the technology in the project.

The technology we are implementing could be see as technical foundation of THEIA project. Handling of data is critical to all other tasks - it is a convergence point for the majority of other activties. The major objective of innovative use of data cubes concept and the use of CREODIAS platform infrastructure is to provide data handling efficiency and security, aligned to modern standards and multidimensional user requirements

Q3.1.
Are you processing or intend to process personal data when developing or using these technologies in THEIA?

Please keep in mind that the terms 'personal data' and 'processing' are rather broad. Processing means the use of personal data at any stage of the Project: collecting, recording, studying and publishing these data, amongst others. Personal data are any information relating to an identified or identifiable natural person. For instance, in THEIA: the processing of a dataset including footage with a camera that records people, the curation of intelligence data from publicly available sources or social media about individuals behaviour, or the collection of information from potential end-users that identify the counterparts, or interaction with them. All these activities imply the processing of personal data, and require an affirmative answer. On the other hand, processing datasets that solely include technical data about UAVs, satellites signal, or geo-spacial resources would not be considered processing of personal data. ***When in doubt, you generally process some personal data. If you have any questions about this, or do not exactly know if you process personal data, please contact MPlegal before continuing with the survey.***

- ( ) Yes
- (•) No

Q3.2.
Please specify the types of personal data which you process.

The categories below are provided for orientation and are not necessarily needed for the purposes of the project. Please specify those relevant to your activities.

This question was not displayed to the respondent.

Q3.3. Develop your previous answer, if it is necessary for any category, or if you clicked "Others".

This question was not displayed to the respondent.

Q3.4.
How will you obtain the personal data?

This question was not displayed to the respondent.

Q3.5. Please specify the sources and means of receiving with regards to all the categories of personal data.

This question was not displayed to the respondent.

Q3.6. Develop and classify per set of personal data the sources.

E.g. Identification data (name and email) are obtained directly from data subjects through a website. Biometric data (facial geometry) are obtained from existing datasets through

This question was not displayed to the respondent.

Q3.7. People need to be informed of the processing of their personal data, unless they are obtained indirecty or anonymised. How do you inform the data subject about the processing activity of personal data?

Please come back to MPlegal with any questions regarding this aspect.

This question was not displayed to the respondent.

Q3.8.
Whose personal data is being processed?

Please describe the data subjects, i.e., the individuals or groups of research participants whose personal data will be collected and processed during the project.

This question was not displayed to the respondent.

Q3.9.
How will you arrange the personal data?

Please describe the datasets of personal data that you have, and map basically your information flows (i.e. what data, where it comes from and where it goes – if it is within your organisation, mention the department; if outside, which partners. **This needs to be a basic answer, which will be developed and used as a base for developing a Data flow map in next deliverables for THEIA.**

This question was not displayed to the respondent.

Q3.10.

What do you want to achieve by collecting the personal data?

Please describe for all the categories of personal data.

This question was not displayed to the respondent.

Q3.11.
How will you use the personal data?

Please describe briefly and precisely for all the categories of personal data.

This question was not displayed to the respondent.

Q3.12.
Is the processing of the personal data really necessary to achieve your purpose?

This question was not displayed to the respondent.

Q3.13. Have you explored alternative means to the use of personal data? (mock data, anonymous dataset, fewer variables of personal data…) How satisfactory would they be to achieve the same outcome?

This question was not displayed to the respondent.

Q3.14.
Where will the personal data be stored?

Please explain the location

This question was not displayed to the respondent.

Q3.15. Where are these servers / storage of personal data?

This question was not displayed to the respondent.

Q3.16.
Will you share the datasets of personal data with third parties, not members of the THEIA consortium?

This question was not displayed to the respondent.

Q3.17.
If yes, please explain the reasons and name the receivers. Please specify if these receivers are located in the European Union or abroad.

This question was not displayed to the respondent.

Q3.18.
Will you cooperate with other partners or external entities for the processing of the personal data?

This question was not displayed to the respondent.

Q3.19.
***If yes**, please specify:*

This question was not displayed to the respondent.

Q3.20.
If you engage with other entities to assist you in data processing, what type of work do they develop? How do you make sure that they comply with data protection principles?
Please describe data types and purposes of joint processing.

This question was not displayed to the respondent.

Q3.21.
Will you work with an external online tool, or other cloud computing solution to process personal data?
If so, which one? Do you know the geographical location for storage of information of such tool or cloud servers (e.g. Europe, US, Canada, Japan)?

This question was not displayed to the respondent.

Q3.22.
In your view, do you think you will need to store the personal data collected for this project after its ending?

Could you please provide a justification, in the light of the purpose for which you process personal data?

This question was not displayed to the respondent.

Q3.23.
Would you be willing to anonymise the data?

Data anonymisation *is a process applied to personal data after which it is no longer possible, now, or in the future, to trace the identity of the individual. It is normally done by separating the elements in the dataset that allow identification. Or assigning random codes of identification to the datasets that cannot be traced back to the original data subject, through encryption.*

This question was not displayed to the respondent.

Q3.24.
***If no**, please provide the reasons.*

This question was not displayed to the respondent.

Q3.25.
Would you be willing to pseudonymise the data?

Pseudonymisation *is a process applied to personal data, replacing the identifiable parts of the dataset with a code or reference number, using an agreed upon code. If you need it, you can reverse the process, and obtain back the individual identity through the used code.*

This question was not displayed to the respondent.

Q3.26.
***If no**, please provide the reasons.*

This question was not displayed to the respondent.

Q3.27. Will you implement data protection by design and by default measures?

Some examples of these measures are providing the control to the data subject over his/her personal data once the technology is implemented. Or reduce the data needed and pseudonymise it.

This question was not displayed to the respondent.

Q3.28.
If yes, develop which ones**. If not**, please provide the reasons.

This question was not displayed to the respondent.

Q3.29.
Will your technology be used for profiling data subjects and/or take automated decisions based solely on the processing of personal data from the data subject? This includes, amongst others, feeding Artificial Intelligence models with the data, in order to obtain decisions over these data subjects.

This question was not displayed to the respondent.

Q3.30. If so, what kind of decisions?

This question was not displayed to the respondent.

Q3.31.
Do you follow or comply with any code of conduct or certification scheme in connection to the processing of personal data? For instance, ISO/IEC 27001:2022 standard for Information security, cybersecurity and privacy protection, Information security management systems; ISO/IEC 42005 Information technology — Artificial intelligence (AI) — AI system impact assessment, or the International Association of Privacy Professionals (IAPP) certifications.

This question was not displayed to the respondent.

Q3.32.
Please identify and provide, if possible, the document or link to the document of certification.

This question was not displayed to the respondent.

Q3.33.
What will be the measures that you will take to secure the personal data that you process?

This question was not displayed to the respondent.

Q3.34.

Data subjects have certain rights under European law regarding the use and processing of their personal data. Do you already have a structure to ensure that data subjects are able to exercise their data subjects rights?

Some examples of these are the right of access to their personal data collected for the purposes of the project, right to erasure such data, right to rectification, right to data portability, possibility for the data subject to withdraw consent. The canalisations of those requests through a Data Protection Officer could be an example of an existing structure.

This question was not displayed to the respondent.

Q3.35.
Please specify technical (e.g. specific email address for requests, software or in-built secure system allowing data subjects to access their own personal data in a transparent way) and organisational measures (e.g. who will provide the information to the data subject) to secure the personal data that you already put in place?

Will you need to limit those data subject rights? If so, please specify which one(s) and the reason to do so.

This question was not displayed to the respondent.

Q3.36. How large is the volume of personal data that you process in the project?

This question was not displayed to the respondent.

Q3.37. Do you process any personal data of children?

Meaning underage people, below the age of 16 years old.

This question was not displayed to the respondent.

Q3.38. Where do you obtain the personal data from children?

i.e. directly from them, from existing datasets, from their parents.

This question was not displayed to the respondent.

Q3.39. If you process personal data from minors, do you contact their parents/legal guardians? What information do you share with them about the data processing?

This question was not displayed to the respondent.

Q3.40. Are third parties involved in the processing of personal data?

This question was not displayed to the respondent.

Q3.41. Who are these third parties? What do they do with the personal data?

This question was not displayed to the respondent.

Q3.42. Please, justify your answer. For instance: we do not process personal data, because all the information that we use in the research project is technical data. Another cause will be that you access personal information, but you cannot identify individuals (anonymisation of personal data). Provide as many details as possible, and examples of the information.

The project scope does not require us to process any personal data - all data we intend to handle is purely technical and/or scientific and comes from project partners. In the case any personal data could be a part of various datasources used by other partners, we expect it to be removed/anonymised before further use (before it falls within our resposibilities).

Q4.1. Do you use existing datasets in your research in the project?

- ○ Yes
- ◉ No

Q4.2. What is the origin of the datasets?

- ○ They were in our possesion before the start of the project.
- ○ They are publicly available.
- ○ We obtained them after the start of the project free of cost.
- ○ We obtained them after the start of the project with a licensing access commercial agreement.
- ◉ I do not know.

Q4.3. Do you consider that the datasets may include personal data in them? Please refer to the information in the previous questions from section 2 about personal data.

- ○ Definitely yes. It is possible to identify individuals within the dataset.
- ○ Definitely yes. The data are anonymised. There is personal information in the dataset, but it is not possible to identify the individual.
- ○ Probably yes.
- ○ Probably no.
- ◉ Definitely no.

Q5.1.
Do you think the use or development of the technology might impact privacy of individuals? (such as migrants, including displaced population due to armed conflicts or climate change, minors, undocumented people, and refugees)

Please keep in mind that privacy might be affected without processing of personal data (for example, drones flying above a private house, satellites capturing metrics of properties and terrain). **If you have any questions about this, or do not exactly know if privacy may be impacted, please contact MPlegal before continuing with the survey.**

- ○ Yes
- ◉ No

◯ Maybe

Q5.2. How does your use or development of the technology potentially impact privacy of individuals?

This question was not displayed to the respondent.

Q5.3.
Is this impact on privacy adequate and necessary to achieve the purpose for the development of this technology? For instance, develop the mission and mandate of a public entity, or provide a technical-tool/research that cannot be developed in any other way.

This question was not displayed to the respondent.

Q5.4. Please explain why.

This question was not displayed to the respondent.

Q5.5.
Are there less invasive solutions that can be used to achieve the same purpose effectively?

This question was not displayed to the respondent.

Q5.6. If yes, which are they, and why are they not used?

This question was not displayed to the respondent.

Q5.7. Do you think the benefits which result from the 'adequate and necessary' (research) activity are higher than the impact that it will cause for the privacy of the user?

This question was not displayed to the respondent.

Q5.8. Please explain why.

This question was not displayed to the respondent.

Q5.9. Does the implementation or use of the technology affect the subjects moral, religious or cultural integrity?

This question was not displayed to the respondent.

Q6.1.
What would be, in your opinion, the benefit for the end-users of the technology and society?

The benefits are in line with Theia general project goals. We provide the modern and efficient techology solution allowing to achieve what we as consortium have promissed/declared in the proposal

Q6.2.
Are there possible safety risks for the subjects related to the use of the technology?

- ○ Yes
- ○ No
- ◉ There might be.

Q6.3. Please, describe them, or justify the negative answer. For instance: there are risks, but we foresee safeguards that reduce them.

It would be not honest to say there are no possible risks at all, but from our point of view any possible risks are somehow typical to all IT inftastructure/data handling activities, and we are well prepared to tackle them - by technology, design and work practices

Q6.4.
What technical and organizational measures can be taken to ensure and increase safety of the technology for end-users and data subjects?

We should and will follow the relevant security/technology standards. These include all the data handling procedures (backup/recovery, consistency checks, infrastructure stability improvement, fail-safe setups, etc.).

Q6.5. Are there any technical and organizational measures which could be taken to increase trust of the society and individuals in the use of the technology?

The most important is to follow the good practices and ensure the maximum system reliability, and then preferably present it through the set of documented KPIs

Q6.6.
Do you foresee any ethical issues related to the development or use of the technology?

- ○ Yes
- ◉ No

Q6.7. Please describe them.

As our activities have mostly/purely technical dimension, we do not oversee any ethical challenges/issues

Q7.1. Are the data used in the project susceptible of misuse? Could they be used, once processed, in a harmful way for the Project or for society?

We do not see at the moment the ways of possible missuse in harmful way, but by design we intend to control the data/system access and monitor the data use.

Q7.2. Are there any measures already implemented which would prevent this misuse to happen?

- (●) Yes
- ( ) No

Q7.3. Detail them or suggest new ones that could be implemented.

The system design includes acces/data control, events logging and system/data use monitoring

Q8.1.
Are there any risks of stigmatisation or discrimination, to your knowledge, in the use of these technologies in GeoAI and law enforcement?

The use of data for law enforcement is a sensitive domain for the general public. Particularly, border surveillance and security raises many societal and ethical questions. The treatment at large scale of information about borders and personal data about migrants needs to be performed in a comprehensive, sensible and protected way. Security measures and responses must be tailored to consider the needs and of vulnerable groups. The potential risk of misinformation must also be considered, as well as the potential generation or amplification of harmful stereotypes concerning these vulnerable groups.

- ( ) Yes
- (●) No

Q8.2. Are there any direct risks of misinformation associated to the use of these technologies?

- ( ) Yes
- (●) No

Q8.3. If any of these risks is spotted, what is the procedure you would follow to minimise and correct the affected stigmatisation or discrimination?

We will immediately take the possible risk mitigation activities (as much as possible within our responsibilities) and report the spotted risk to all consortium members

Q9.1. THEIA project has endeavoured to develop the research with attention to gender, inclusion, and adequate social norms. This requires not to consider, and not to inflict any negative gender stereotypes. The creation or propagation of gender stereotypes could lead to issues of discrimination for particular genders, or

worsen other problematic already existing, and potential discrimination. Could the use of the technology help in tackling these stereotypes?

- (●) Yes
- ( ) No

Q9.2. How does it do so?

The design and planned activities are innovative and stereotypes agnostic. In fact we do not see any discrimination possibilities in all project scope and especially in relation to our activities.

Q9.3. Are there any risks of amplification of gender issues in the use of your technology, or development of your research in the project? Please describe them.

We do not see any risks of this kind - all our planned activities are gender agnostic.

Q10.1.
If you consider that an important point has not been asked or you would like to make a comment for feedback, please type it down here.

THANK YOU FOR ANSWERING THE QUESTIONS!

Q1.1. Which type of organisation do you represent in the Project?

- ○ End user
- ◉ Project partner
- ○ Stakeholder

Q1.2. Type-in the name of your organisation or the partner you represent in THEIA project

Creotech

Q1.3.
Please, type-in your name.

Your name will not be shared with anyone, neither with the other partners of the Consortium, nor published with the survey. It will only be used if internal checking of the results, or feedback is needed by MPLegal.

Q2.1.
Which technology or process is developed or used by your organisation in the project?

- ☑ Data processing pathway
- ☐ Users requirements coordination, demo activities and use-cases
- ☐ Very-High-Resolution Earth Observation tools (Thermal imaging and low-visibility sensing)
- ☐ Very-High-Resolution Earth Observation tools (Data acquisition: Space-based video)
- ☑ Very-High-Resolution Earth Observation tools (Data acquisition: Satellite-Based Multi-Payload Data)
- ☐ Data acquisition: Micro-satellites & Cubesats
- ☐ Data acquisition: UAS-based data
- ☑ Integration of the multi-sensor platform
- ☐ Testing sensors on drones. Drones deployment for testing in real conditions
- ☐ AI for detecting and tracking objects
- ☐ THEIA crowdsourcing tool
- ☐ Database for the Areas of Interest
- ☐ High-velocity transnational data
- ☐ Data fusion & Data models. Data exchange framework

- [ ] Data exchange platform for cloud infrastructure to satellite data
- [ ] National Constellation Data Federation
- [ ] Optimized API Access
- [ ] GeoAI. UAS and terrestrial sensor-based image processing
- [ ] GeoAI. Georeferencing
- [ ] GeoAI. Intelligence Gathering
- [ ] GeoAI. Fusion and GeoAI Module
- [ ] THEIA platform
- [x] Demonstration and validation activities
- [ ] Communication, Dissemination, Training and Exploitation
- [ ] Others

Q2.2. If Others, please specify which ones, and within which Work Package in the project.

Q2.3. Briefly describe the objectives and possible benefits of the development and use of the technology in the project.

Providing efficient access to relevant data resources of the EU Copernicus Program and federation of the available national constellations data.

Q3.1.
Are you processing or intend to process personal data when developing or using these technologies in THEIA?

Please keep in mind that the terms 'personal data' and 'processing' are rather broad. Processing means the use of personal data at any stage of the Project: collecting, recording, studying and publishing these data, amongst others. Personal data are any information relating to an identified or identifiable natural person. For instance, in THEIA: the processing of a dataset including footage with a camera that records people, the curation of intelligence data from publicly available sources or social media about individuals behaviour, or the collection of information from potential end-users that identify the counterparts, or interaction with them. All these activities imply the processing of personal data, and require an affirmative answer. On the other hand, processing datasets that solely include technical data about UAVs, satellites signal, or geo-spacial resources would not be considered processing of personal data. ***When in doubt, you generally process some personal data. If you have any questions about this, or do not exactly know if you process personal data, please contact MPlegal before continuing with the survey.***

- ( ) Yes
- (•) No

Q3.2.
Please specify the types of personal data which you process.

The categories below are provided for orientation and are not necessarily needed for the purposes of the project. Please specify those relevant to your activities.

This question was not displayed to the respondent.

Q3.3. Develop your previous answer, if it is necessary for any category, or if you clicked "Others".

This question was not displayed to the respondent.

Q3.4.
How will you obtain the personal data?

This question was not displayed to the respondent.

Q3.5. Please specify the sources and means of receiving with regards to all the categories of personal data.

This question was not displayed to the respondent.

Q3.6. Develop and classify per set of personal data the sources.

E.g. Identification data (name and email) are obtained directly from data subjects through a website. Biometric data (facial geometry) are obtained from existing datasets through

This question was not displayed to the respondent.

Q3.7. People need to be informed of the processing of their personal data, unless they are obtained indirecty or anonymised. How do you inform the data subject about the processing activity of personal data?

Please come back to MPlegal with any questions regarding this aspect.

This question was not displayed to the respondent.

Q3.8.
Whose personal data is being processed?

Please describe the data subjects, i.e., the individuals or groups of research participants whose personal data will be collected and processed during the project.

This question was not displayed to the respondent.

Q3.9.
How will you arrange the personal data?

Please describe the datasets of personal data that you have, and map basically your information flows (i.e. what data, where it comes from and where it goes – if it is within your organisation, mention the department; if outside, which partners. **This needs to be a basic answer, which will be developed and used as a base for developing a Data flow map in next deliverables for THEIA.**

This question was not displayed to the respondent.

Q3.10.

What do you want to achieve by collecting the personal data?

Please describe for all the categories of personal data.

This question was not displayed to the respondent.

Q3.11.
How will you use the personal data?

Please describe briefly and precisely for all the categories of personal data.

This question was not displayed to the respondent.

Q3.12.
Is the processing of the personal data really necessary to achieve your purpose?

This question was not displayed to the respondent.

Q3.13. Have you explored alternative means to the use of personal data? (mock data, anonymous dataset, fewer variables of personal data…) How satisfactory would they be to achieve the same outcome?

This question was not displayed to the respondent.

Q3.14.
Where will the personal data be stored?

Please explain the location

This question was not displayed to the respondent.

Q3.15. Where are these servers / storage of personal data?

This question was not displayed to the respondent.

Q3.16.
Will you share the datasets of personal data with third parties, not members of the THEIA consortium?

This question was not displayed to the respondent.

Q3.17.
If yes, please explain the reasons and name the receivers. Please specify if these receivers are located in the European Union or abroad.

This question was not displayed to the respondent.

Q3.18.
Will you cooperate with other partners or external entities for the processing of the personal data?

This question was not displayed to the respondent.

Q3.19.
***If yes**, please specify:*

This question was not displayed to the respondent.

Q3.20.
If you engage with other entities to assist you in data processing, what type of work do they develop? How do you make sure that they comply with data protection principles?
Please describe data types and purposes of joint processing.

This question was not displayed to the respondent.

Q3.21.
Will you work with an external online tool, or other cloud computing solution to process personal data?
If so, which one? Do you know the geographical location for storage of information of such tool or cloud servers (e.g. Europe, US, Canada, Japan)?

This question was not displayed to the respondent.

Q3.22.
In your view, do you think you will need to store the personal data collected for this project after its ending?

Could you please provide a justification, in the light of the purpose for which you process personal data?

This question was not displayed to the respondent.

Q3.23.
Would you be willing to anonymise the data?

Data anonymisation *is a process applied to personal data after which it is no longer possible, now, or in the future, to trace the identity of the individual. It is normally done by separating the elements in the dataset that allow identification. Or assigning random codes of identification to the datasets that cannot be traced back to the original data subject, through encryption.*

This question was not displayed to the respondent.

Q3.24.
***If no**, please provide the reasons.*

This question was not displayed to the respondent.

Q3.25.
Would you be willing to pseudonymise the data?

Pseudonymisation *is a process applied to personal data, replacing the identifiable parts of the dataset with a code or reference number, using an agreed upon code. If you need it, you can reverse the process, and obtain back the individual identity through the used code.*

This question was not displayed to the respondent.

Q3.26.
***If no**, please provide the reasons.*

This question was not displayed to the respondent.

Q3.27. Will you implement data protection by design and by default measures?

Some examples of these measures are providing the control to the data subject over his/her personal data once the technology is implemented. Or reduce the data needed and pseudonymise it.

This question was not displayed to the respondent.

Q3.28.
If yes, develop which ones**. If not**, please provide the reasons.

This question was not displayed to the respondent.

Q3.29.
Will your technology be used for profiling data subjects and/or take automated decisions based solely on the processing of personal data from the data subject? This includes, amongst others, feeding Artificial Intelligence models with the data, in order to obtain decisions over these data subjects.

This question was not displayed to the respondent.

Q3.30. If so, what kind of decisions?

This question was not displayed to the respondent.

Q3.31.
Do you follow or comply with any code of conduct or certification scheme in connection to the processing of personal data? For instance, ISO/IEC 27001:2022 standard for Information security, cybersecurity and privacy protection, Information security management systems; ISO/IEC 42005 Information technology — Artificial intelligence (AI) — AI system impact assessment, or the International Association of Privacy Professionals (IAPP) certifications.

This question was not displayed to the respondent.

Q3.32.
Please identify and provide, if possible, the document or link to the document of certification.

This question was not displayed to the respondent.

Q3.33.
What will be the measures that you will take to secure the personal data that you process?

This question was not displayed to the respondent.

Q3.34.

Data subjects have certain rights under European law regarding the use and processing of their personal data. Do you already have a structure to ensure that data subjects are able to exercise their data subjects rights?

Some examples of these are the right of access to their personal data collected for the purposes of the project, right to erasure such data, right to rectification, right to data portability, possibility for the data subject to withdraw consent. The canalisations of those requests through a Data Protection Officer could be an example of an existing structure.

This question was not displayed to the respondent.

Q3.35.
Please specify technical (e.g. specific email address for requests, software or in-built secure system allowing data subjects to access their own personal data in a transparent way) and organisational measures (e.g. who will provide the information to the data subject) to secure the personal data that you already put in place?

Will you need to limit those data subject rights? If so, please specify which one(s) and the reason to do so.

This question was not displayed to the respondent.

Q3.36. How large is the volume of personal data that you process in the project?

This question was not displayed to the respondent.

Q3.37. Do you process any personal data of children?

Meaning underage people, below the age of 16 years old.

This question was not displayed to the respondent.

Q3.38. Where do you obtain the personal data from children?

i.e. directly from them, from existing datasets, from their parents.

This question was not displayed to the respondent.

Q3.39. If you process personal data from minors, do you contact their parents/legal guardians? What information do you share with them about the data processing?

This question was not displayed to the respondent.

Q3.40. Are third parties involved in the processing of personal data?

This question was not displayed to the respondent.

Q3.41. Who are these third parties? What do they do with the personal data?

This question was not displayed to the respondent.

Q3.42. Please, justify your answer. For instance: we do not process personal data, because all the information that we use in the research project is technical data. Another cause will be that you access personal information, but you cannot identify individuals (anonymisation of personal data). Provide as many details as possible, and examples of the information.

We do not process personal data, because all the information that we use in the research project is technical data. All data are publically available datasets coming from EU or national EO data sources / programs.

Q4.1. Do you use existing datasets in your research in the project?

- (●) Yes
- ( ) No

Q4.2. What is the origin of the datasets?

- ( ) They were in our possesion before the start of the project.
- (●) They are publicly available.
- ( ) We obtained them after the start of the project free of cost.
- ( ) We obtained them after the start of the project with a licensing access commercial agreement.
- ( ) I do not know.

Q4.3. Do you consider that the datasets may include personal data in them? Please refer to the information in the previous questions from section 2 about personal data.

- ( ) Definitely yes. It is possible to identify individuals within the dataset.
- ( ) Definitely yes. The data are anonymised. There is personal information in the dataset, but it is not possible to identify the individual.
- ( ) Probably yes.
- ( ) Probably no.
- (●) Definitely no.

Q5.1.
Do you think the use or development of the technology might impact privacy of individuals? (such as migrants, including displaced population due to armed conflicts or climate change, minors, undocumented people, and refugees)

Please keep in mind that privacy might be affected without processing of personal data (for example, drones flying above a private house, satellites capturing metrics of properties and terrain). **If you have any questions about this, or do not exactly know if privacy may be impacted, please contact MPlegal before continuing with the survey.**

- ( ) Yes
- (●) No

◯ Maybe

Q5.2. How does your use or development of the technology potentially impact privacy of individuals?

This question was not displayed to the respondent.

Q5.3.
Is this impact on privacy adequate and necessary to achieve the purpose for the development of this technology? For instance, develop the mission and mandate of a public entity, or provide a technical-tool/research that cannot be developed in any other way.

This question was not displayed to the respondent.

Q5.4. Please explain why.

This question was not displayed to the respondent.

Q5.5.
Are there less invasive solutions that can be used to achieve the same purpose effectively?

This question was not displayed to the respondent.

Q5.6. If yes, which are they, and why are they not used?

This question was not displayed to the respondent.

Q5.7. Do you think the benefits which result from the ‘adequate and necessary’ (research) activity are higher than the impact that it will cause for the privacy of the user?

This question was not displayed to the respondent.

Q5.8. Please explain why.

This question was not displayed to the respondent.

Q5.9. Does the implementation or use of the technology affect the subjects moral, religious or cultural integrity?

This question was not displayed to the respondent.

Q6.1.
What would be, in your opinion, the benefit for the end-users of the technology and society?

This question was not displayed to the respondent.

Q6.2.

Are there possible safety risks for the subjects related to the use of the technology?

This question was not displayed to the respondent.

Q6.3. Please, describe them, or justify the negative answer. For instance: there are risks, but we foresee safeguards that reduce them.

This question was not displayed to the respondent.

Q6.4.
What technical and organizational measures can be taken to ensure and increase safety of the technology for end-users and data subjects?

This question was not displayed to the respondent.

Q6.5. Are there any technical and organizational measures which could be taken to increase trust of the society and individuals in the use of the technology?

This question was not displayed to the respondent.

Q6.6.
Do you foresee any ethical issues related to the development or use of the technology?

This question was not displayed to the respondent.

Q6.7. Please describe them.

This question was not displayed to the respondent.

Q7.1. Are the data used in the project susceptible of misuse? Could they be used, once processed, in a harmful way for the Project or for society?

This question was not displayed to the respondent.

Q7.2. Are there any measures already implemented which would prevent this misuse to happen?

This question was not displayed to the respondent.

Q7.3. Detail them or suggest new ones that could be implemented.

This question was not displayed to the respondent.

Q8.1.
Are there any risks of stigmatisation or discrimination, to your knowledge, in the use of these technologies in GeoAI and law enforcement?

The use of data for law enforcement is a sensitive domain for the general public. Particularly, border surveillance and security raises many societal and ethical questions. The treatment at large scale of information about borders and personal data about migrants needs to be performed in a comprehensive, sensible and protected way. Security measures and responses must be tailored to consider the needs and of

vulnerable groups. The potential risk of misinformation must also be considered, as well as the potential generation or amplification of harmful stereotypes concerning these vulnerable groups.

This question was not displayed to the respondent.

Q8.2. Are there any direct risks of misinformation associated to the use of these technologies?

This question was not displayed to the respondent.

Q8.3. If any of these risks is spotted, what is the procedure you would follow to minimise and correct the affected stigmatisation or discrimination?

This question was not displayed to the respondent.

Q9.1. THEIA project has endeavoured to develop the research with attention to gender, inclusion, and adequate social norms. This requires not to consider, and not to inflict any negative gender stereotypes. The creation or propagation of gender stereotypes could lead to issues of discrimination for particular genders, or worsen other problematic already existing, and potential discrimination. Could the use of the technology help in tackling these stereotypes?

This question was not displayed to the respondent.

Q9.2. How does it do so?

This question was not displayed to the respondent.

Q9.3. Are there any risks of amplification of gender issues in the use of your technology, or development of your research in the project? Please describe them.

This question was not displayed to the respondent.

Q10.1.
If you consider that an important point has not been asked or you would like to make a comment for feedback, please type it down here.

THANK YOU FOR ANSWERING THE QUESTIONS!

This question was not displayed to the respondent.

Q1.1. Which type of organisation do you represent in the Project?

- ○ End user
- ◉ Project partner
- ○ Stakeholder

Q1.2. Type-in the name of your organisation or the partner you represent in THEIA project

C3I Intelligent Systems Ltd

Q1.3.
Please, type-in your name.

Your name will not be shared with anyone, neither with the other partners of the Consortium, nor published with the survey. It will only be used if internal checking of the results, or feedback is needed by MPLegal.

Q2.1.
Which technology or process is developed or used by your organisation in the project?

- ☐ Data processing pathway
- ☐ Users requirements coordination, demo activities and use-cases
- ☐ Very-High-Resolution Earth Observation tools (Thermal imaging and low-visibility sensing)
- ☐ Very-High-Resolution Earth Observation tools (Data acquisition: Space-based video)
- ☐ Very-High-Resolution Earth Observation tools (Data acquisition: Satellite-Based Multi-Payload Data)
- ☐ Data acquisition: Micro-satellites & Cubesats
- ☑ Data acquisition: UAS-based data
- ☐ Integration of the multi-sensor platform
- ☑ Testing sensors on drones. Drones deployment for testing in real conditions
- ☐ AI for detecting and tracking objects
- ☐ THEIA crowdsourcing tool
- ☐ Database for the Areas of Interest
- ☐ High-velocity transnational data
- ☐ Data fusion & Data models. Data exchange framework

- [ ] Data exchange platform for cloud infrastructure to satellite data
- [ ] National Constellation Data Federation
- [ ] Optimized API Access
- [ ] GeoAI. UAS and terrestrial sensor-based image processing
- [ ] GeoAI. Georeferencing
- [ ] GeoAI. Intelligence Gathering
- [ ] GeoAI. Fusion and GeoAI Module
- [ ] THEIA platform
- [ ] Demonstration and validation activities
- [ ] Communication, Dissemination, Training and Exploitation
- [ ] Others

Q2.2. If Others, please specify which ones, and within which Work Package in the project.

Q2.3. Briefly describe the objectives and possible benefits of the development and use of the technology in the project.

Drone-based aerial imagery is used to support monitoring of operational environments and to test and validate project technologies. The use of this technology improves situational awareness and supports more effective planning and response during operational scenarios.

Q3.1.
Are you processing or intend to process personal data when developing or using these technologies in THEIA?

Please keep in mind that the terms 'personal data' and 'processing' are rather broad. Processing means the use of personal data at any stage of the Project: collecting, recording, studying and publishing these data, amongst others. Personal data are any information relating to an identified or identifiable natural person. For instance, in THEIA: the processing of a dataset including footage with a camera that records people, the curation of intelligence data from publicly available sources or social media about individuals behaviour, or the collection of information from potential end-users that identify the counterparts, or interaction with them. All these activities imply the processing of personal data, and require an affirmative answer. On the other hand, processing datasets that solely include technical data about UAVs, satellites signal, or geo-spacial resources would not be considered processing of personal data. ***When in doubt, you generally process some personal data. If you have any questions about this, or do not exactly know if you process personal data, please contact MPlegal before continuing with the survey.***

- ○ Yes
- ◉ No

Q3.2.
Please specify the types of personal data which you process.

The categories below are provided for orientation and are not necessarily needed for the purposes of the project. Please specify those relevant to your activities.

This question was not displayed to the respondent.

Q3.3. Develop your previous answer, if it is necessary for any category, or if you clicked "Others".

This question was not displayed to the respondent.

Q3.4.
How will you obtain the personal data?

This question was not displayed to the respondent.

Q3.5. Please specify the sources and means of receiving with regards to all the categories of personal data.

This question was not displayed to the respondent.

Q3.6. Develop and classify per set of personal data the sources.

E.g. Identification data (name and email) are obtained directly from data subjects through a website. Biometric data (facial geometry) are obtained from existing datasets through

This question was not displayed to the respondent.

Q3.7. People need to be informed of the processing of their personal data, unless they are obtained indirecty or anonymised. How do you inform the data subject about the processing activity of personal data?

Please come back to MPlegal with any questions regarding this aspect.

This question was not displayed to the respondent.

Q3.8.
Whose personal data is being processed?

Please describe the data subjects, i.e., the individuals or groups of research participants whose personal data will be collected and processed during the project.

This question was not displayed to the respondent.

Q3.9.
How will you arrange the personal data?

Please describe the datasets of personal data that you have, and map basically your information flows (i.e. what data, where it comes from and where it goes – if it is within your organisation, mention the department; if outside, which partners. **This needs to be a basic answer, which will be developed and used as a base for developing a Data flow map in next deliverables for THEIA.**

This question was not displayed to the respondent.

Q3.10.

What do you want to achieve by collecting the personal data?

Please describe for all the categories of personal data.

This question was not displayed to the respondent.

Q3.11.
How will you use the personal data?

Please describe briefly and precisely for all the categories of personal data.

This question was not displayed to the respondent.

Q3.12.
Is the processing of the personal data really necessary to achieve your purpose?

This question was not displayed to the respondent.

Q3.13. Have you explored alternative means to the use of personal data? (mock data, anonymous dataset, fewer variables of personal data…) How satisfactory would they be to achieve the same outcome?

This question was not displayed to the respondent.

Q3.14.
Where will the personal data be stored?

Please explain the location

This question was not displayed to the respondent.

Q3.15. Where are these servers / storage of personal data?

This question was not displayed to the respondent.

Q3.16.
Will you share the datasets of personal data with third parties, not members of the THEIA consortium?

This question was not displayed to the respondent.

Q3.17.
If yes, please explain the reasons and name the receivers. Please specify if these receivers are located in the European Union or abroad.

This question was not displayed to the respondent.

Q3.18.
Will you cooperate with other partners or external entities for the processing of the personal data?

This question was not displayed to the respondent.

Q3.19.
***If yes**, please specify:*

This question was not displayed to the respondent.

Q3.20.
If you engage with other entities to assist you in data processing, what type of work do they develop? How do you make sure that they comply with data protection principles?
Please describe data types and purposes of joint processing.

This question was not displayed to the respondent.

Q3.21.
Will you work with an external online tool, or other cloud computing solution to process personal data?
If so, which one? Do you know the geographical location for storage of information of such tool or cloud servers (e.g. Europe, US, Canada, Japan)?

This question was not displayed to the respondent.

Q3.22.
In your view, do you think you will need to store the personal data collected for this project after its ending?

Could you please provide a justification, in the light of the purpose for which you process personal data?

This question was not displayed to the respondent.

Q3.23.
Would you be willing to anonymise the data?

Data anonymisation *is a process applied to personal data after which it is no longer possible, now, or in the future, to trace the identity of the individual. It is normally done by separating the elements in the dataset that allow identification. Or assigning random codes of identification to the datasets that cannot be traced back to the original data subject, through encryption.*

This question was not displayed to the respondent.

Q3.24.
***If no**, please provide the reasons.*

This question was not displayed to the respondent.

Q3.25.
Would you be willing to pseudonymise the data?

Pseudonymisation *is a process applied to personal data, replacing the identifiable parts of the dataset with a code or reference number, using an agreed upon code. If you need it, you can reverse the process, and obtain back the individual identity through the used code.*

This question was not displayed to the respondent.

Q3.26.
***If no**, please provide the reasons.*

This question was not displayed to the respondent.

Q3.27. Will you implement data protection by design and by default measures?

Some examples of these measures are providing the control to the data subject over his/her personal data once the technology is implemented. Or reduce the data needed and pseudonymise it.

This question was not displayed to the respondent.

Q3.28.
If yes, develop which ones**. If not**, please provide the reasons.

This question was not displayed to the respondent.

Q3.29.
Will your technology be used for profiling data subjects and/or take automated decisions based solely on the processing of personal data from the data subject? This includes, amongst others, feeding Artificial Intelligence models with the data, in order to obtain decisions over these data subjects.

This question was not displayed to the respondent.

Q3.30. If so, what kind of decisions?

This question was not displayed to the respondent.

Q3.31.
Do you follow or comply with any code of conduct or certification scheme in connection to the processing of personal data? For instance, ISO/IEC 27001:2022 standard for Information security, cybersecurity and privacy protection, Information security management systems; ISO/IEC 42005 Information technology — Artificial intelligence (AI) — AI system impact assessment, or the International Association of Privacy Professionals (IAPP) certifications.

This question was not displayed to the respondent.

Q3.32.
Please identify and provide, if possible, the document or link to the document of certification.

This question was not displayed to the respondent.

Q3.33.
What will be the measures that you will take to secure the personal data that you process?

This question was not displayed to the respondent.

Q3.34.

Data subjects have certain rights under European law regarding the use and processing of their personal data. Do you already have a structure to ensure that data subjects are able to exercise their data subjects rights?

Some examples of these are the right of access to their personal data collected for the purposes of the project, right to erasure such data, right to rectification, right to data portability, possibility for the data subject to withdraw consent. The canalisations of those requests through a Data Protection Officer could be an example of an existing structure.

This question was not displayed to the respondent.

Q3.35.
Please specify technical (e.g. specific email address for requests, software or in-built secure system allowing data subjects to access their own personal data in a transparent way) and organisational measures (e.g. who will provide the information to the data subject) to secure the personal data that you already put in place?

Will you need to limit those data subject rights? If so, please specify which one(s) and the reason to do so.

This question was not displayed to the respondent.

Q3.36. How large is the volume of personal data that you process in the project?

This question was not displayed to the respondent.

Q3.37. Do you process any personal data of children?

Meaning underage people, below the age of 16 years old.

This question was not displayed to the respondent.

Q3.38. Where do you obtain the personal data from children?

i.e. directly from them, from existing datasets, from their parents.

This question was not displayed to the respondent.

Q3.39. If you process personal data from minors, do you contact their parents/legal guardians? What information do you share with them about the data processing?

This question was not displayed to the respondent.

Q3.40. Are third parties involved in the processing of personal data?

This question was not displayed to the respondent.

Q3.41. Who are these third parties? What do they do with the personal data?

This question was not displayed to the respondent.

Q3.42. Please, justify your answer. For instance: we do not process personal data, because all the information that we use in the research project is technical data. Another cause will be that you access personal information, but you cannot identify individuals (anonymisation of personal data). Provide as many details as possible, and examples of the information.

The technologies used by C3I in the context of THEIA involve the collection of aerial imagery through drone platforms for monitoring and operational testing purposes. The data collected consists of environmental and technical information related to operational scenarios and infrastructure. No personal data is collected, processed or analysed, and the system is not used to identify individuals. Therefore, the activities carried out by C3I within the project do not involve the processing of personal data.

Q4.1. Do you use existing datasets in your research in the project?

- (●) Yes
- ( ) No

Q4.2. What is the origin of the datasets?

- ( ) They were in our possesion before the start of the project.
- (●) They are publicly available.
- ( ) We obtained them after the start of the project free of cost.
- ( ) We obtained them after the start of the project with a licensing access commercial agreement.
- ( ) I do not know.

Q4.3. Do you consider that the datasets may include personal data in them? Please refer to the information in the previous questions from section 2 about personal data.

- ( ) Definitely yes. It is possible to identify individuals within the dataset.
- ( ) Definitely yes. The data are anonymised. There is personal information in the dataset, but it is not possible to identify the individual.
- ( ) Probably yes.
- ( ) Probably no.
- (●) Definitely no.

Q5.1.
Do you think the use or development of the technology might impact privacy of individuals? (such as migrants, including displaced population due to armed conflicts or climate change, minors, undocumented people, and refugees)

Please keep in mind that privacy might be affected without processing of personal data (for example, drones flying above a private house, satellites capturing metrics of properties and terrain). **If you have any questions about this, or do not exactly know if privacy may be impacted, please contact MPlegal before continuing with the survey.**

- ( ) Yes
- ( ) No

- (●) Maybe

Q5.2. How does your use or development of the technology potentially impact privacy of individuals?

The use of drone-based aerial imagery may theoretically raise privacy considerations when operating over inhabited or privately owned areas. However, the activities carried out within the project do not aim to identify individuals. The collected imagery focuses on environmental and operational information for testing and validation of the project technologies. No personal data is intentionally collected or processed and appropriate operational measures are applied to minimise any potential privacy impact

Q5.3.
Is this impact on privacy adequate and necessary to achieve the purpose for the development of this technology? For instance, develop the mission and mandate of a public entity, or provide a technical-tool/research that cannot be developed in any other way.

- (●) Yes
- ( ) No

Q5.4. Please explain why.

The limited potential impact on privacy is considered necessary and proportionate to achieve the objectives of the technology. Drone-based aerial imagery is required to support monitoring of operational environments and to test and validate the project technologies. The project does not aim to identify individuals and no personal data is intentionally collected or processed. Operational measures are applied to minimise any potential privacy impact.

Q5.5.
Are there less invasive solutions that can be used to achieve the same purpose effectively?

- ( ) Yes
- (●) No

Q5.6. If yes, which are they, and why are they not used?

Q5.7. Do you think the benefits which result from the ‘adequate and necessary’ (research) activity are higher than the impact that it will cause for the privacy of the user?

- (●) Definitely Higher
- ( ) Proportionate
- ( ) Non-proportionate
- ( ) Lower

Q5.8. Please explain why.

The expected benefits of the technology are significantly higher than the potential impact on privacy. Drone-based aerial imagery supports improved situational awareness, monitoring of operational environments and validation of project technologies. The activities do not aim to identify individuals and no personal data is intentionally collected or processed. Appropriate operational measures are applied to minimise any potential privacy impact.

Q5.9. Does the implementation or use of the technology affect the subjects moral, religious or cultural integrity?

- ○ Yes
- ◉ No

Q6.1.
What would be, in your opinion, the benefit for the end-users of the technology and society?

The technology can provide significant benefits for end-users by improving situational awareness, monitoring capabilities and operational decision-making in complex environments. The use of drone-based aerial imagery supports faster and more effective assessment of situations and helps authorities and operational actors respond more efficiently. For society, the technology can contribute to improved safety, better management of emergencies and enhanced protection of critical infrastructures and the environment

Q6.2.
Are there possible safety risks for the subjects related to the use of the technology?

- ○ Yes
- ○ No
- ◉ There might be.

Q6.3. Please, describe them, or justify the negative answer. For instance: there are risks, but we foresee safeguards that reduce them.

There may be limited operational safety risks associated with the use of drone platforms, such as technical malfunction or operational incidents. However, these risks are mitigated through established safety procedures, trained operators, and compliance with applicable aviation regulations. The technology is used in controlled operational environments and appropriate safeguards are applied to ensure safe deployment.

Q6.4.
What technical and organizational measures can be taken to ensure and increase safety of the technology for end-users and data subjects?

Safety can be ensured through the use of trained and certified drone operators, compliance with applicable aviation and safety regulations, and the use of reliable and tested drone platforms. Operational procedures, risk assessments and pre-flight checks are applied before each deployment. In addition, the technology is used in controlled operational environments and appropriate data management practices are followed to ensure secure handling of the collected information.

Q6.5. Are there any technical and organizational measures which could be taken to increase trust of the society and individuals in the use of the technology?

Trust can be increased through transparency in the use of the technology, clear communication of its objectives and benefits, and compliance with applicable legal and ethical frameworks. The implementation of privacy-by-design principles, responsible data management practices and clear operational guidelines can further strengthen public confidence in the technology

Q6.6.
Do you foresee any ethical issues related to the development or use of the technology?

- ○ Yes
- ◉ No

Q6.7. Please describe them.

Q7.1. Are the data used in the project susceptible of misuse? Could they be used, once processed, in a harmful way for the Project or for society?

The data used within the project mainly consist of aerial imagery and technical information collected for research and operational testing purposes. These data do not include personal data and are not intended to identify individuals. Therefore, the risk of misuse is considered very limited. In addition, appropriate data management and access control measures are applied within the project to ensure that the data are used only for legitimate research and operational purposes

Q7.2. Are there any measures already implemented which would prevent this misuse to happen?

- ◉ Yes
- ○ No

Q7.3. Detail them or suggest new ones that could be implemented.

Several measures are implemented to prevent potential misuse of the data. These include controlled access to project data, the use of the information strictly for research and operational testing purposes, and compliance with applicable legal and ethical frameworks. In addition, data management procedures and internal project guidelines ensure that the collected information is handled responsibly and only by authorised project partners.

Q8.1.
Are there any risks of stigmatisation or discrimination, to your knowledge, in the use of these technologies in GeoAI and law enforcement?

The use of data for law enforcement is a sensitive domain for the general public. Particularly, border surveillance and security raises many societal and ethical questions. The treatment at large scale of information about borders and personal data about migrants needs to be performed in a comprehensive, sensible and protected way. Security measures and responses must be tailored to consider the needs and of vulnerable groups. The potential risk of misinformation must also be considered, as well as the potential generation or amplification of harmful stereotypes concerning these vulnerable groups.

- (●) Yes
- ( ) No

Q8.2. Are there any direct risks of misinformation associated to the use of these technologies?

- ( ) Yes
- (●) No

Q8.3. If any of these risks is spotted, what is the procedure you would follow to minimise and correct the affected stigmatisation or discrimination?

Q9.1. THEIA project has endeavoured to develop the research with attention to gender, inclusion, and adequate social norms. This requires not to consider, and not to inflict any negative gender stereotypes. The creation or propagation of gender stereotypes could lead to issues of discrimination for particular genders, or worsen other problematic already existing, and potential discrimination. Could the use of the technology help in tackling these stereotypes?

- (●) Yes
- ( ) No

Q9.2. How does it do so?

The technology does not process personal data or profile individuals and therefore does not target or discriminate against any gender group. Its use focuses on environmental and operational monitoring and supports decision-making processes that are neutral and applicable to all individuals. By ensuring responsible and unbiased use of technology, the project contributes to avoiding the creation or reinforcement of gender stereotypes

Q9.3. Are there any risks of amplification of gender issues in the use of your technology, or development of your research in the project? Please describe them.

No specific risks of amplifying gender-related issues are foreseen. The technology developed in the project focuses on environmental and operational monitoring and does not involve profiling, categorisation or analysis of individuals based on gender or other personal characteristics.

Q10.1.
If you consider that an important point has not been asked or you would like to make a comment for feedback, please type it down here.

THANK YOU FOR ANSWERING THE QUESTIONS!

The project activities described in this questionnaire focus on operational testing and environmental monitoring and do not involve the processing of personal data or the identification of individuals. All activities are carried out in compliance with applicable legal, ethical and safety frameworks.

Q1.1. Which type of organisation do you represent in the Project?

- ○ End user
- ◉ Project partner
- ○ Stakeholder

Q1.2. Type-in the name of your organisation or the partner you represent in THEIA project

WEB-TO-CLIMATE WTOC

Q1.3.
Please, type-in your name.

Your name will not be shared with anyone, neither with the other partners of the Consortium, nor published with the survey. It will only be used if internal checking of the results, or feedback is needed by MPLegal.

Q2.1.
Which technology or process is developed or used by your organisation in the project?

- ☐ Data processing pathway
- ☐ Users requirements coordination, demo activities and use-cases
- ☐ Very-High-Resolution Earth Observation tools (Thermal imaging and low-visibility sensing)
- ☐ Very-High-Resolution Earth Observation tools (Data acquisition: Space-based video)
- ☐ Very-High-Resolution Earth Observation tools (Data acquisition: Satellite-Based Multi-Payload Data)
- ☐ Data acquisition: Micro-satellites & Cubesats
- ☐ Data acquisition: UAS-based data
- ☐ Integration of the multi-sensor platform
- ☐ Testing sensors on drones. Drones deployment for testing in real conditions
- ☐ AI for detecting and tracking objects
- ☑ THEIA crowdsourcing tool
- ☐ Database for the Areas of Interest
- ☐ High-velocity transnational data
- ☐ Data fusion & Data models. Data exchange framework

- [ ] Data exchange platform for cloud infrastructure to satellite data
- [ ] National Constellation Data Federation
- [ ] Optimized API Access
- [ ] GeoAI. UAS and terrestrial sensor-based image processing
- [ ] GeoAI. Georeferencing
- [ ] GeoAI. Intelligence Gathering
- [ ] GeoAI. Fusion and GeoAI Module
- [ ] THEIA platform
- [ ] Demonstration and validation activities
- [ ] Communication, Dissemination, Training and Exploitation
- [ ] Others

Q2.2. If Others, please specify which ones, and within which Work Package in the project.

Q2.3. Briefly describe the objectives and possible benefits of the development and use of the technology in the project.

We implement advanced techniques to improve the accuracy and relevance of information gathered from crowdsourced contributions and open-source data, always keeping GDPR and ethical principles in mind. Integrate a multi-source extraction framework, drawing from a diverse pool of publicly available sources including social media platforms to enrich the dataset with a wide spectrum of perspectives and information. The main benefit by our contribution is to propose significant changes in the way security risks are identified, analysed, and mitigated by leveraging the untapped potential of crowdsourcing and open-source data. This innovative approach will provide a richer, more comprehensive understanding of security challenges, enabling more effective responses and fostering a more informed and resilient community.

Q3.1.
Are you processing or intend to process personal data when developing or using these technologies in THEIA?

Please keep in mind that the terms 'personal data' and 'processing' are rather broad. Processing means the use of personal data at any stage of the Project: collecting, recording, studying and publishing these data, amongst others. Personal data are any information relating to an identified or identifiable natural person. For instance, in THEIA: the processing of a dataset including footage with a camera that records people, the curation of intelligence data from publicly available sources or social media about individuals behaviour, or the collection of information from potential end-users that identify the counterparts, or interaction with them. All these activities imply the processing of personal data, and require an affirmative answer. On the other hand, processing datasets that solely include technical data about UAVs, satellites signal, or geo-spacial resources would not be considered processing of personal data. ***When in doubt, you generally process some personal data. If you have any questions about this, or do not exactly know if you process personal data, please contact MPlegal before continuing with the survey.***

- ○ Yes
- ◉ No

Q3.2.

Please specify the types of personal data which you process.

The categories below are provided for orientation and are not necessarily needed for the purposes of the project. Please specify those relevant to your activities.

This question was not displayed to the respondent.

Q3.3. Develop your previous answer, if it is necessary for any category, or if you clicked "Others".

This question was not displayed to the respondent.

Q3.4.
How will you obtain the personal data?

This question was not displayed to the respondent.

Q3.5. Please specify the sources and means of receiving with regards to all the categories of personal data.

This question was not displayed to the respondent.

Q3.6. Develop and classify per set of personal data the sources.

E.g. Identification data (name and email) are obtained directly from data subjects through a website. Biometric data (facial geometry) are obtained from existing datasets through

This question was not displayed to the respondent.

Q3.7. People need to be informed of the processing of their personal data, unless they are obtained indirecty or anonymised. How do you inform the data subject about the processing activity of personal data?

Please come back to MPlegal with any questions regarding this aspect.

This question was not displayed to the respondent.

Q3.8.
Whose personal data is being processed?

Please describe the data subjects, i.e., the individuals or groups of research participants whose personal data will be collected and processed during the project.

This question was not displayed to the respondent.

Q3.9.
How will you arrange the personal data?

Please describe the datasets of personal data that you have, and map basically your information flows (i.e. what data, where it comes from and where it goes – if it is within your organisation, mention the department; if outside, which partners. **This needs to be a basic answer, which will be developed and used as a base for developing a Data flow map in next deliverables for THEIA.**

This question was not displayed to the respondent.

Q3.10.
What do you want to achieve by collecting the personal data?

Please describe for all the categories of personal data.

This question was not displayed to the respondent.

Q3.11.
How will you use the personal data?

Please describe briefly and precisely for all the categories of personal data.

This question was not displayed to the respondent.

Q3.12.
Is the processing of the personal data really necessary to achieve your purpose?

This question was not displayed to the respondent.

Q3.13. Have you explored alternative means to the use of personal data? (mock data, anonymous dataset, fewer variables of personal data…) How satisfactory would they be to achieve the same outcome?

This question was not displayed to the respondent.

Q3.14.
Where will the personal data be stored?

Please explain the location

This question was not displayed to the respondent.

Q3.15. Where are these servers / storage of personal data?

This question was not displayed to the respondent.

Q3.16.
Will you share the datasets of personal data with third parties, not members of the THEIA consortium?

This question was not displayed to the respondent.

Q3.17.
If yes, please explain the reasons and name the receivers. Please specify if these receivers are located in the European Union or abroad.

This question was not displayed to the respondent.

Q3.18.
Will you cooperate with other partners or external entities for the processing of the personal data?

This question was not displayed to the respondent.

Q3.19.
***If yes**, please specify:*

This question was not displayed to the respondent.

Q3.20.
If you engage with other entities to assist you in data processing, what type of work do they develop? How do you make sure that they comply with data protection principles?
Please describe data types and purposes of joint processing.

This question was not displayed to the respondent.

Q3.21.
Will you work with an external online tool, or other cloud computing solution to process personal data?
If so, which one? Do you know the geographical location for storage of information of such tool or cloud servers (e.g. Europe, US, Canada, Japan)?

This question was not displayed to the respondent.

Q3.22.
In your view, do you think you will need to store the personal data collected for this project after its ending?

Could you please provide a justification, in the light of the purpose for which you process personal data?

This question was not displayed to the respondent.

Q3.23.
Would you be willing to anonymise the data?

Data anonymisation *is a process applied to personal data after which it is no longer possible, now, or in the future, to trace the identity of the individual. It is normally done by separating the elements in the dataset that allow identification. Or assigning random codes of identification to the datasets that cannot be traced back to the original data subject, through encryption.*

This question was not displayed to the respondent.

Q3.24.
***If no**, please provide the reasons.*

This question was not displayed to the respondent.

Q3.25.
Would you be willing to pseudonymise the data?

Pseudonymisation *is a process applied to personal data, replacing the identifiable parts of the dataset with a code or reference number, using an agreed upon code. If you need it, you can reverse the process, and obtain back the individual identity through the used code.*

This question was not displayed to the respondent.

Q3.26.
***If no**, please provide the reasons.*

This question was not displayed to the respondent.

Q3.27. Will you implement data protection by design and by default measures?

Some examples of these measures are providing the control to the data subject over his/her personal data once the technology is implemented. Or reduce the data needed and pseudonymise it.

This question was not displayed to the respondent.

Q3.28.
If yes, develop which ones**. If not**, please provide the reasons.

This question was not displayed to the respondent.

Q3.29.
Will your technology be used for profiling data subjects and/or take automated decisions based solely on the processing of personal data from the data subject? This includes, amongst others, feeding Artificial Intelligence models with the data, in order to obtain decisions over these data subjects.

This question was not displayed to the respondent.

Q3.30. If so, what kind of decisions?

This question was not displayed to the respondent.

Q3.31.
Do you follow or comply with any code of conduct or certification scheme in connection to the processing of personal data? For instance, ISO/IEC 27001:2022 standard for Information security, cybersecurity and privacy protection, Information security management systems; ISO/IEC 42005 Information technology — Artificial intelligence (AI) — AI system impact assessment, or the International Association of Privacy Professionals (IAPP) certifications.

This question was not displayed to the respondent.

Q3.32.
Please identify and provide, if possible, the document or link to the document of certification.

This question was not displayed to the respondent.

Q3.33.
What will be the measures that you will take to secure the personal data that you process?

This question was not displayed to the respondent.

Q3.34.
Data subjects have certain rights under European law regarding the use and processing of their personal data. Do you already have a structure to ensure that data subjects are able to exercise their data subjects rights?

Some examples of these are the right of access to their personal data collected for the purposes of the project, right to erasure such data, right to rectification, right to data portability, possibility for the data subject to withdraw consent. The canalisations of those requests through a Data Protection Officer could be an example of an existing structure.

This question was not displayed to the respondent.

Q3.35.
Please specify technical (e.g. specific email address for requests, software or in-built secure system allowing data subjects to access their own personal data in a transparent way) and organisational measures (e.g. who will provide the information to the data subject) to secure the personal data that you already put in place?

Will you need to limit those data subject rights? If so, please specify which one(s) and the reason to do so.

This question was not displayed to the respondent.

Q3.36. How large is the volume of personal data that you process in the project?

This question was not displayed to the respondent.

Q3.37. Do you process any personal data of children?

Meaning underage people, below the age of 16 years old.

This question was not displayed to the respondent.

Q3.38. Where do you obtain the personal data from children?

i.e. directly from them, from existing datasets, from their parents.

This question was not displayed to the respondent.

Q3.39. If you process personal data from minors, do you contact their parents/legal guardians? What information do you share with them about the data processing?

This question was not displayed to the respondent.

Q3.40. Are third parties involved in the processing of personal data?

This question was not displayed to the respondent.

Q3.41. Who are these third parties? What do they do with the personal data?

This question was not displayed to the respondent.

Q3.42. Please, justify your answer. For instance: we do not process personal data, because all the information that we use in the research project is technical data. Another cause will be that you access personal information, but you cannot identify individuals (anonymisation of personal data). Provide as many details as possible, and examples of the information.

Our deliverable functions solely as a stateless processing and forwarding component, handling only non-personal data and ensuring that no personal or sensitive information is collected, stored, or retained at any point in the workflow. During the execution of our processes, no personal data is captured, stored, or retained by our tool at any stage. The system is designed to operate without collecting information that could directly or indirectly identify an individual. All data processed by our tool is non-personal in nature. No personally identifiable information (PII), such as names, email addresses, usernames, IP addresses linked to individuals, device identifiers, or authentication data is collected or processed. Any information generated during processing will be transmitted exclusively via secure APIs to the THEIA platform for further analysis and correlation. The data is not stored locally or persistently within our environment. Once transmission is completed, no residual data remains within the tool. As a result: The tool cannot be used to identify individuals, either directly or through data correlation. There is no data persistence, logging, or historical storage of processed information. The architecture supports data minimization and privacy-by-design principles, aligning with applicable data protection requirements (e.g., GDPR).

Q4.1. Do you use existing datasets in your research in the project?

- (●) Yes
- ( ) No

Q4.2. What is the origin of the datasets?

- (●) They were in our possesion before the start of the project.
- ( ) They are publicly available.
- ( ) We obtained them after the start of the project free of cost.
- ( ) We obtained them after the start of the project with a licensing access commercial agreement.
- ( ) I do not know.

Q4.3. Do you consider that the datasets may include personal data in them? Please refer to the information in the previous questions from section 2 about personal data.

- ( ) Definitely yes. It is possible to identify individuals within the dataset.
- ( ) Definitely yes. The data are anonymised. There is personal information in the dataset, but it is not possible to identify the individual.
- ( ) Probably yes.
- ( ) Probably no.
- (●) Definitely no.

Q5.1.
Do you think the use or development of the technology might impact privacy of individuals? (such as migrants, including displaced population due to armed conflicts or climate change, minors, undocumented people, and refugees)

Please keep in mind that privacy might be affected without processing of personal data (for example, drones flying above a private house, satellites capturing metrics of properties and terrain). **If you have any**

questions about this, or do not exactly know if privacy may be impacted, please contact MPlegal before continuing with the survey.

- ○ Yes
- ◉ No
- ○ Maybe

Q5.2. How does your use or development of the technology potentially impact privacy of individuals?

This question was not displayed to the respondent.

Q5.3.
Is this impact on privacy adequate and necessary to achieve the purpose for the development of this technology? For instance, develop the mission and mandate of a public entity, or provide a technical-tool/research that cannot be developed in any other way.

This question was not displayed to the respondent.

Q5.4. Please explain why.

This question was not displayed to the respondent.

Q5.5.
Are there less invasive solutions that can be used to achieve the same purpose effectively?

This question was not displayed to the respondent.

Q5.6. If yes, which are they, and why are they not used?

This question was not displayed to the respondent.

Q5.7. Do you think the benefits which result from the 'adequate and necessary' (research) activity are higher than the impact that it will cause for the privacy of the user?

This question was not displayed to the respondent.

Q5.8. Please explain why.

This question was not displayed to the respondent.

Q5.9. Does the implementation or use of the technology affect the subjects moral, religious or cultural integrity?

This question was not displayed to the respondent.

Q6.1.
What would be, in your opinion, the benefit for the end-users of the technology and society?

Provide a richer, more comprehensive understanding of security challenges, enabling more effective responses and fostering a more informed and resilient community.

Q6.2.
Are there possible safety risks for the subjects related to the use of the technology?

- ○ Yes
- ◉ No
- ○ There might be.

Q6.3. Please, describe them, or justify the negative answer. For instance: there are risks, but we foresee safeguards that reduce them.

No safety risks occur from our tool.

Q6.4.
What technical and organizational measures can be taken to ensure and increase safety of the technology for end-users and data subjects?

Strict authentication mechanisms and restricted access to data with role based access control.

Q6.5. Are there any technical and organizational measures which could be taken to increase trust of the society and individuals in the use of the technology?

Clear and thorough description of the project objectives and usage. Open access to regular reports or data for informing the public of the results achieved throughout the project.

Q6.6.
Do you foresee any ethical issues related to the development or use of the technology?

- ○ Yes
- ◉ No

Q6.7. Please describe them.

Q7.1. Are the data used in the project susceptible of misuse? Could they be used, once processed, in a harmful way for the Project or for society?

Every technology can be used in a harmful way. It is the responsibility of everyone to use the technology in an ethical way and without contradicting human rights.

Q7.2. Are there any measures already implemented which would prevent this misuse to happen?

- ○ Yes
- ◉ No

Q7.3. Detail them or suggest new ones that could be implemented.

Q8.1.
Are there any risks of stigmatisation or discrimination, to your knowledge, in the use of these technologies in GeoAI and law enforcement?

The use of data for law enforcement is a sensitive domain for the general public. Particularly, border surveillance and security raises many societal and ethical questions. The treatment at large scale of information about borders and personal data about migrants needs to be performed in a comprehensive, sensible and protected way. Security measures and responses must be tailored to consider the needs and of vulnerable groups. The potential risk of misinformation must also be considered, as well as the potential generation or amplification of harmful stereotypes concerning these vulnerable groups.

- ◉ Yes
- ○ No

Q8.2. Are there any direct risks of misinformation associated to the use of these technologies?

- ◉ Yes
- ○ No

Q8.3. If any of these risks is spotted, what is the procedure you would follow to minimise and correct the affected stigmatisation or discrimination?

As the project evolves the algorithms can be reevaluated to mitigate the risk of misinformation.

Q9.1. THEIA project has endeavoured to develop the research with attention to gender, inclusion, and adequate social norms. This requires not to consider, and not to inflict any negative gender stereotypes. The creation or propagation of gender stereotypes could lead to issues of discrimination for particular genders, or worsen other problematic already existing, and potential discrimination. Could the use of the technology help in tackling these stereotypes?

- (●) Yes
- ( ) No

Q9.2. How does it do so?

The technology developed and employed within this project does not rely on gender-based attributes, classifications, or assumptions, nor does it incorporate demographic profiling that could lead to biased outcomes. By operating on gender-neutral, non-personal, and objective data, the technology minimizes the risk of introducing or perpetuating gender bias within its processes or outputs.

Q9.3. Are there any risks of amplification of gender issues in the use of your technology, or development of your research in the project? Please describe them.

The risk of amplification of gender-related issues in the use of the technology or in the development of the research is considered low to negligible, due to the nature of the system and the safeguards embedded in the project design. The technology does not collect, process, or infer gender-related attributes, nor does it rely on personal, demographic, or behavioral profiling that could introduce gender bias. All processing is performed on non-personal, technical, and gender-neutral data, which significantly limits the possibility of reproducing or amplifying existing gender inequalities or stereotypes.

Q10.1.
If you consider that an important point has not been asked or you would like to make a comment for feedback, please type it down here.

THANK YOU FOR ANSWERING THE QUESTIONS!

Q1.1. Which type of organisation do you represent in the Project?

- ○ End user
- ◉ Project partner
- ○ Stakeholder

Q1.2. Type-in the name of your organisation or the partner you represent in THEIA project

MPLegal

Q1.3.
Please, type-in your name.

Your name will not be shared with anyone, neither with the other partners of the Consortium, nor published with the survey. It will only be used if internal checking of the results, or feedback is needed by MPLegal.

Q2.1.
Which technology or process is developed or used by your organisation in the project?

- ☐ Data processing pathway
- ☐ Users requirements coordination, demo activities and use-cases
- ☐ Very-High-Resolution Earth Observation tools (Thermal imaging and low-visibility sensing)
- ☐ Very-High-Resolution Earth Observation tools (Data acquisition: Space-based video)
- ☐ Very-High-Resolution Earth Observation tools (Data acquisition: Satellite-Based Multi-Payload Data)
- ☐ Data acquisition: Micro-satellites & Cubesats
- ☐ Data acquisition: UAS-based data
- ☐ Integration of the multi-sensor platform
- ☐ Testing sensors on drones. Drones deployment for testing in real conditions
- ☐ AI for detecting and tracking objects
- ☐ THEIA crowdsourcing tool
- ☐ Database for the Areas of Interest
- ☐ High-velocity transnational data
- ☐ Data fusion & Data models. Data exchange framework

- [ ] Data exchange platform for cloud infrastructure to satellite data
- [ ] National Constellation Data Federation
- [ ] Optimized API Access
- [ ] GeoAI. UAS and terrestrial sensor-based image processing
- [ ] GeoAI. Georeferencing
- [ ] GeoAI. Intelligence Gathering
- [ ] GeoAI. Fusion and GeoAI Module
- [ ] THEIA platform
- [ ] Demonstration and validation activities
- [x] Communication, Dissemination, Training and Exploitation
- [x] Others

Q2.2. If Others, please specify which ones, and within which Work Package in the project.

Work Package 3 on Ethics.

Q2.3. Briefly describe the objectives and possible benefits of the development and use of the technology in the project.

The goal is to ensure compliance with laws and regulations to mitigate risks. Establish and follow-up clear guidelines within the space sector, upholding ethics, GDPR compliance, and legal support for integrity.

Q3.1.
Are you processing or intend to process personal data when developing or using these technologies in THEIA?

Please keep in mind that the terms 'personal data' and 'processing' are rather broad. Processing means the use of personal data at any stage of the Project: collecting, recording, studying and publishing these data, amongst others. Personal data are any information relating to an identified or identifiable natural person. For instance, in THEIA: the processing of a dataset including footage with a camera that records people, the curation of intelligence data from publicly available sources or social media about individuals behaviour, or the collection of information from potential end-users that identify the counterparts, or interaction with them. All these activities imply the processing of personal data, and require an affirmative answer. On the other hand, processing datasets that solely include technical data about UAVs, satellites signal, or geo-spacial resources would not be considered processing of personal data. ***When in doubt, you generally process some personal data. If you have any questions about this, or do not exactly know if you process personal data, please contact MPlegal before continuing with the survey.***

- (●) Yes
- ( ) No

Q3.2.
Please specify the types of personal data which you process.

The categories below are provided for orientation and are not necessarily needed for the purposes of the project. Please specify those relevant to your activities.

- [x] a) Identification data (e.g. name, data of birth, age, gender, address, email, phone number)
- [ ] b) Personal features
- [ ] c) Financial data
- [ ] d) Physical, physiological or behavioural characteristics, of a natural person, allowing his/her identification.
- [ ] e) Genetic data
- [ ] f) Biometric data
- [ ] g) Other information regarding health, incl. mental health
- [ ] h) Habits
- [ ] i) Family composition
- [ ] j) Hobbies and interests
- [ ] k) Consumption patterns
- [ ] l) Residence or home address
- [ ] m) Education
- [x] n) Occupation, employment or professional affiliation
- [ ] o) Social security number or other national identification codes (Passport or ID number)
- [ ] p) Racial or ethnic background
- [ ] q) Philosophical or spiritual orientation
- [ ] r) Information on sexual preferences
- [ ] s) Political orientation or opinion
- [ ] t) Membership of trade union or affiliation
- [ ] u) Other memberships
- [ ] v) Video footage of individuals
- [ ] w) Others

Q3.3. Develop your previous answer, if it is necessary for any category, or if you clicked "Others".

Generally, we process personal data of the researchers in the project, such as contact emails, to reach them and pose questions about ethical aspects of the project. Incidentally, we may have access to personal data processed by the rest of the partners in the project through the project repository, reports and deliverables of the project.

Q3.4.
How will you obtain the personal data?

- [x] Directly from data subjects
- [x] Other partners
- [ ] Other sources
- [ ] I do not know

Q3.5. Please specify the sources and means of receiving with regards to all the categories of personal data.

- [ ] Sensors
- [ ] Video recordings
- [ ] Software
- [ ] Website
- [x] Questionnaires
- [x] Existing datasets
- [x] Other means
- [ ] I do not know

Q3.6. Develop and classify per set of personal data the sources.

E.g. Identification data (name and email) are obtained directly from data subjects through a website. Biometric data (facial geometry) are obtained from existing datasets through

Identification data are obtained directly from the data subjects (the researchers in the project) via direct communications and questionnaires. Other personal data may be accessed indirectly through the project repository.

Q3.7. People need to be informed of the processing of their personal data, unless they are obtained indirecty or anonymised. How do you inform the data subject about the processing activity of personal data?

Please come back to MPlegal with any questions regarding this aspect.

For the personal data from the project researchers, the processing is limited, and always in direct communication with them, via email, internet or phone calls. As recipients of the personal data, we do not directly contact the data subjects. We only access the information to the extent allowed by the other partners in the project.

Q3.8.
Whose personal data is being processed?

Please describe the data subjects, i.e., the individuals or groups of research participants whose personal data will be collected and processed during the project.

Researchers in the project. Any other data subject whose personal data is included by other partners in the project repository.

Q3.9.
How will you arrange the personal data?

Please describe the datasets of personal data that you have, and map basically your information flows (i.e. what data, where it comes from and where it goes – if it is within your organisation, mention the department; if outside, which partners. **This needs to be a basic answer, which will be developed and used as a base for developing a Data flow map in next deliverables for THEIA.**

The only datasets that we store are the already available in the repository of the project, thorugh mailing lists and lists of contacts. We do not extract that information, and only access it directly in the project repository.

Q3.10.
What do you want to achieve by collecting the personal data?

Please describe for all the categories of personal data.

Solely the clear communication in the project. The rest of access to the data is incidental, and not directly related to our research in the project.

Q3.11.
How will you use the personal data?

Please describe briefly and precisely for all the categories of personal data.

To contact the researchers in the project, to the extent necessary for the development of the research.

Q3.12.
Is the processing of the personal data really necessary to achieve your purpose?

- (●) Essential
- ( ) Important
- ( ) Accessory
- ( ) Not necessary

Q3.13. Have you explored alternative means to the use of personal data? (mock data, anonymous dataset, fewer variables of personal data…) How satisfactory would they be to achieve the same outcome?

- ( ) No, I have not explored them.
- (●) Yes, I know them. They would not be effective for the purpose.
- ( ) Yes, I know them. They are currently under use.
- ( ) No, we have not explored them. We will incorporate them in the future.

Q3.14.
Where will the personal data be stored?

Please explain the location

- [ ] Locally, in corporate servers, including those accessible remotely via cloud.

- [ ] Locally, in corporate devices.
- [x] Cloud
- [ ] Third parties servers
- [ ] Other

Q3.15. Where are these servers / storage of personal data?

- (•) In a country member of the European Union
- ( ) In a country outside the European Union
- ( ) Unknown

Q3.16.
Will you share the datasets of personal data with third parties, not members of the THEIA consortium?

- ( ) Yes
- (•) No

Q3.17.
If yes, please explain the reasons and name the receivers. Please specify if these receivers are located in the European Union or abroad.

N/A

Q3.18.
Will you cooperate with other partners or external entities for the processing of the personal data?

- ( ) Yes
- (•) No

Q3.19.
***If yes**, please specify:*

- ( ) We need the cooperation as assisting in our processing activities, and for our own purposes.
- ( ) We negotiate and control together the collaboration. We define jointly the purposes of the processing.
- ( ) Other engagement.

Q3.20.
If you engage with other entities to assist you in data processing, what type of work do they develop? How do you make sure that they comply with data protection principles?
Please describe data types and purposes of joint processing.

We do not engage with third parties for the processing of the personal data.

Q3.21.
Will you work with an external online tool, or other cloud computing solution to process personal data?
If so, which one? Do you know the geographical location for storage of information of such tool or cloud servers (e.g. Europe, US, Canada, Japan)?

The project repository is hosted in Microsoft Dropbox. The data stored there, to our knowledge is in servers within European Union territory.

Q3.22.
In your view, do you think you will need to store the personal data collected for this project after its ending?

Could you please provide a justification, in the light of the purpose for which you process personal data?

No, we will not need to retain the personal data after the end of the project.

Q3.23.
Would you be willing to anonymise the data?

Data anonymisation *is a process applied to personal data after which it is no longer possible, now, or in the future, to trace the identity of the individual. It is normally done by separating the elements in the dataset that allow identification. Or assigning random codes of identification to the datasets that cannot be traced back to the original data subject, through encryption.*

- ○ Yes
- ◉ No

Q3.24.
***If no**, please provide the reasons.*

We do not have direct control of the project repository, where the data are stored.

Q3.25.
Would you be willing to pseudonymise the data?

Pseudonymisation *is a process applied to personal data, replacing the identifiable parts of the dataset with a code or reference number, using an agreed upon code. If you need it, you can reverse the process, and obtain back the individual identity through the used code.*

- (●) Yes
- ( ) No

Q3.26.
***If no**, please provide the reasons.*

N/A

Q3.27. Will you implement data protection by design and by default measures?

Some examples of these measures are providing the control to the data subject over his/her personal data once the technology is implemented. Or reduce the data needed and pseudonymise it.

- ( ) Yes
- (●) No

Q3.28.
If yes, develop which ones**. If not**, please provide the reasons.

The processing of the personal data is very limited. These measures would be disproportionate to the goal of the processing, which is solely direct communications.

Q3.29.
Will your technology be used for profiling data subjects and/or take automated decisions based solely on the processing of personal data from the data subject? This includes, amongst others, feeding Artificial Intelligence models with the data, in order to obtain decisions over these data subjects.

- ( ) Yes
- (●) No

Q3.30. If so, what kind of decisions?

N/A

Q3.31.
Do you follow or comply with any code of conduct or certification scheme in connection to the processing of personal data? For instance, ISO/IEC 27001:2022 standard for Information security, cybersecurity and

privacy protection, Information security management systems; ISO/IEC 42005 Information technology — Artificial intelligence (AI) — AI system impact assessment, or the International Association of Privacy Professionals (IAPP) certifications.

- ○ Yes
- ◉ No

Q3.32.
Please identify and provide, if possible, the document or link to the document of certification.

N/A

Q3.33.
What will be the measures that you will take to secure the personal data that you process?

Emails and contacts are not stored locally. Only in the respositories of the project. We follow the security measures foreseen for the access to the project repository. The devices that we use to access the repository are protected with passwords and stored safely in our premises.

Q3.34.
Data subjects have certain rights under European law regarding the use and processing of their personal data. Do you already have a structure to ensure that data subjects are able to exercise their data subjects rights?

Some examples of these are the right of access to their personal data collected for the purposes of the project, right to erasure such data, right to rectification, right to data portability, possibility for the data subject to withdraw consent. The canalisations of those requests through a Data Protection Officer could be an example of an existing structure.

- ○ Yes
- ◉ No

Q3.35.
Please specify technical (e.g. specific email address for requests, software or in-built secure system allowing data subjects to access their own personal data in a transparent way) and organisational measures (e.g. who will provide the information to the data subject) to secure the personal data that you already put in place?

Will you need to limit those data subject rights? If so, please specify which one(s) and the reason to do so.

N/A

Q3.36. How large is the volume of personal data that you process in the project?

- (●) Small
- ( ) Large
- ( ) Not processing any personal data

Q3.37. Do you process any personal data of children?

Meaning underage people, below the age of 16 years old.

- (●) Definitely not
- ( ) Probably not
- ( ) Probably yes
- ( ) Definitely yes

Q3.38. Where do you obtain the personal data from children?

i.e. directly from them, from existing datasets, from their parents.

N/A

Q3.39. If you process personal data from minors, do you contact their parents/legal guardians? What information do you share with them about the data processing?

N/A

Q3.40. Are third parties involved in the processing of personal data?

- (●) No.
- ( ) Yes, as contractors, performing some specific tasks under our instructions.
- ( ) Yes, we grant them access to the personal data.
- ( ) Yes, they have the same control over the data that we have.
- ( ) Yes, but we do not know the details.

Q3.41. Who are these third parties? What do they do with the personal data?

N/A

Q3.42. Please, justify your answer. For instance: we do not process personal data, because all the information that we use in the research project is technical data. Another cause will be that you access personal information, but you cannot identify individuals (anonymisation of personal data). Provide as many details as possible, and examples of the information.

This question was not displayed to the respondent.

Q4.1. Do you use existing datasets in your research in the project?

- ○ Yes
- ◉ No

Q4.2. What is the origin of the datasets?

- ○ They were in our possesion before the start of the project.
- ○ They are publicly available.
- ○ We obtained them after the start of the project free of cost.
- ○ We obtained them after the start of the project with a licensing access commercial agreement.
- ◉ I do not know.

Q4.3. Do you consider that the datasets may include personal data in them? Please refer to the information in the previous questions from section 2 about personal data.

- ○ Definitely yes. It is possible to identify individuals within the dataset.
- ○ Definitely yes. The data are anonymised. There is personal information in the dataset, but it is not possible to identify the individual.
- ○ Probably yes.
- ○ Probably no.
- ◉ Definitely no.

Q5.1.
Do you think the use or development of the technology might impact privacy of individuals? (such as migrants, including displaced population due to armed conflicts or climate change, minors, undocumented people, and refugees)

Please keep in mind that privacy might be affected without processing of personal data (for example, drones flying above a private house, satellites capturing metrics of properties and terrain). **If you have any questions about this, or do not exactly know if privacy may be impacted, please contact MPlegal before continuing with the survey.**

- ○ Yes
- ◉ No
- ○ Maybe

Q5.2. How does your use or development of the technology potentially impact privacy of individuals?

This question was not displayed to the respondent.

Q5.3.
Is this impact on privacy adequate and necessary to achieve the purpose for the development of this technology? For instance, develop the mission and mandate of a public entity, or provide a technical-tool/research that cannot be developed in any other way.

This question was not displayed to the respondent.

Q5.4. Please explain why.

This question was not displayed to the respondent.

Q5.5.
Are there less invasive solutions that can be used to achieve the same purpose effectively?

This question was not displayed to the respondent.

Q5.6. If yes, which are they, and why are they not used?

This question was not displayed to the respondent.

Q5.7. Do you think the benefits which result from the 'adequate and necessary' (research) activity are higher than the impact that it will cause for the privacy of the user?

This question was not displayed to the respondent.

Q5.8. Please explain why.

This question was not displayed to the respondent.

Q5.9. Does the implementation or use of the technology affect the subjects moral, religious or cultural integrity?

This question was not displayed to the respondent.

Q6.1.
What would be, in your opinion, the benefit for the end-users of the technology and society?

The benefit of our research in the project is to introduce and oversee compliance with the existing legal framework for space research, privacy, data protection and other ethical aspects. The content of the research for THEIA project needs to be designed in such a way. End-users will have access to better tools to develop their work and fulfill their missions. Society will benefit from safer borders, better attention to migrants and other displaced population.

Q6.2.

Are there possible safety risks for the subjects related to the use of the technology?

- (●) Yes
- ( ) No
- ( ) There might be.

Q6.3. Please, describe them, or justify the negative answer. For instance: there are risks, but we foresee safeguards that reduce them.

There may be risks for privacy and data protection of the migrants and displaced population under surveillance, once the technologies developed in THEIA are deployed in real-use cases. The development of the technologies is done considering those potential risks for a privacy-by-desing system.

Q6.4.
What technical and organizational measures can be taken to ensure and increase safety of the technology for end-users and data subjects?

Information access and empowering individuals with control over their own personal data.

Q6.5. Are there any technical and organizational measures which could be taken to increase trust of the society and individuals in the use of the technology?

Public disclosure of the use of the technologies by end-users.

Q6.6.
Do you foresee any ethical issues related to the development or use of the technology?

- ( ) Yes
- (●) No

Q6.7. Please describe them.

N/A

Q7.1. Are the data used in the project susceptible of misuse? Could they be used, once processed, in a harmful way for the Project or for society?

It is highly unlikely. The data that we process are contact information such as emails and professional affiliation. They are, in many cases available publicly. The impact of misuse would be minimal.

Q7.2. Are there any measures already implemented which would prevent this misuse to happen?

- (●) Yes
- ( ) No

Q7.3. Detail them or suggest new ones that could be implemented.

Limit access to the information via the project repository, and only to researchers in the project.

Q8.1.
Are there any risks of stigmatisation or discrimination, to your knowledge, in the use of these technologies in GeoAI and law enforcement?

The use of data for law enforcement is a sensitive domain for the general public. Particularly, border surveillance and security raises many societal and ethical questions. The treatment at large scale of information about borders and personal data about migrants needs to be performed in a comprehensive, sensible and protected way. Security measures and responses must be tailored to consider the needs and of vulnerable groups. The potential risk of misinformation must also be considered, as well as the potential generation or amplification of harmful stereotypes concerning these vulnerable groups.

- (●) Yes
- ( ) No

Q8.2. Are there any direct risks of misinformation associated to the use of these technologies?

- (●) Yes
- ( ) No

Q8.3. If any of these risks is spotted, what is the procedure you would follow to minimise and correct the affected stigmatisation or discrimination?

Informing the individuals to the extent possible of the processing of their personal information. Empower them with the tools to manage their own personal data. Diclose the use of these tools by end-users to the general public.

Q9.1. THEIA project has endeavoured to develop the research with attention to gender, inclusion, and adequate social norms. This requires not to consider, and not to inflict any negative gender stereotypes. The creation or propagation of gender stereotypes could lead to issues of discrimination for particular genders, or worsen other problematic already existing, and potential discrimination. Could the use of the technology help in tackling these stereotypes?

- ( ) Yes

◉ No

Q9.2. How does it do so?

N/A

Q9.3. Are there any risks of amplification of gender issues in the use of your technology, or development of your research in the project? Please describe them.

N/A

Q10.1.
If you consider that an important point has not been asked or you would like to make a comment for feedback, please type it down here.

THANK YOU FOR ANSWERING THE QUESTIONS!

END OF DOCUMENT