D7.1 Requirement no.1
Ethics

Funded by
the European Union

D7.1 – Requirement no 1 Ethics

Grant Agreement number	101070162
Project title	Ultimate
Project start date	1 October 2022
Duration	36 months

Work package	WP7
Due date	30.09.2023
Submission date	4 October 2023
Deliverable lead	CBR
Authors	Irina Marsh (CBR)
Contributors	-
Reviewers	Julien Perouelle (LNE)

Abstract

Deliverable D7.1 elaborates on the ethical requirements imposed by the EU Commission on the ULTIMATE project as part of the Grant Agreement 101070162: "*The ethics advisor should ensure that the rights of the workers are preserved concerning privacy and data protection and that they are truly free to accept or reject participation to the research experiment in WP5"*.
Deliverable D7.1 offers the argument that a Data Protection Impact Assessment (DPIA) doesn't need to be conducted (section 2) based on the requirements and the guidance provided by GDPR and consulting normative sources. In section 3 the document describes the technical and organisational measures which are implemented in ULTIMATE in order to protect the privacy and data protection rights of data subjects and research participants in WP5 Demonstrators: UC2 - Robotic workshop (PIAP) and UC3 – Industry: Robotic arms (ROB), including the compliance statements of PIAP and ROB DPO's and the support and approval letter from the External Ethical Expert (in the annex 5).

Document revision history

Version	Date	Description of change	Contributor(s)
v0.1	21.09.2023	First version	Irina Marsh (CBR)
v0.2	25.09.2023	Text (review, modifications etc)	Julien Perouelle (LNE), Michel Barreteau (TRT)
v1.0	30.09.2023	Final version	Irina Marsh (CBR) Dominic Kelly (CBR)

Project co-funded by the European Commission in the Horizon Europe programme

Nature of the deliverable *	ETHICS
Dissemination level	PU

Table of contents

List of tables

Abbreviations

DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EEA	External Ethics Advisor
GDPR	General Data Protection Regulation
PEO	Project Ethics Officer
UC	Use Case
WP	Work Package

Executive summary

This document has been submitted for the purpose of meeting the ethical requirements imposed on the ULTIMATE project as part of the Grant Agreement 101070162. These ethical requirements were provided by the European Commission after the approval of the project's funding. They are reflected in the ULTIMATE Grant Agreement and final version of the Division of Actions. As a section of Work Package 7 ("Ethics Requirements"), the consortium must hereon draft and submit Deliverable 7.1 ("Requirement No.1") with the following description: The "Hybrid AI for Robotic navigation and collaborative work" demonstrator considers the detection and precise tracking of the human workers. The ethics advisor should ensure that the rights of the workers are preserved concerning privacy and data protection and that they are truly free to accept or reject participation to the research experiment. A first report on this topic should be provided before the start of WP5 (M12)".

The D7.1 offers the argument that a Data Protection Impact Assessment (DPIA) doesn't need to be conducted (section 2) based on the requirements and the guidance provided by GDPR and consulting normative sources. In section 3 the document describes the technical and organisational measures which are implemented in ULTIMATE in order to protect the privacy and data protection rights of data subjects and research participants in WP5 Demonstrators: UC2 - Robotic workshop (PIAP) and UC3 – Industry: Robotic arms (ROB), including compliance statements of PIAP and ROB DPO's and the support and approval letter from the External Ethical Expert (in the annexes).

The project coordinator, TRT, has overall responsibility of the implementations of these measures with support from Project Ethics Officer (PEO) from CBR and under the guidance of the External Ethics Advisor (EEA).

1. Introduction

1.1. ULTIMATE project

ULTIMATE project is funded by the Horizon Europe framework of the EU, under the thematic area of: *A human centred and ethical development of digital and industrial technologies 2021 (Horizon-CL42021-Human-01)*, coordinated by Thales (TRT), France.

The Project's Coordinator is Dr. Michel Barreteau (TRT). The Data Protection Officer (DPO) is Dr. Gaëlle Lortal (TRT). The Project's Ethics Officer (PEO) is Dr. Irina Marsh (CBR). The primary ethics partner within the consortium is CBR. The full list of consortium partners is available below:

No	Name	Short Name	Country
1	THALES S.A.	TRT	France
2	ROBOTNIK AUTOMATION SLL	ROB	Spain
3	KUNGLIGA TEKNISKA HOEGSKOLAN	KTH	Sweden
4	LABORATOIRE NATIONAL DE METROLOGIE ET D ESSAIS	LNE	France
5	FUNDACION TECNALIA RESEARCH & INNOVATION	TEC	Spain
6	SIEC BADAWCZA LUKASIEWICZ - PRZEMYSLOWY INSTYTUT AUTOMATYKI I POMIAROW PIAP	PIAP	Poland
7	ITTI SP ZOO	ITTI	Poland
8	THALES ALENIA SPACE FRANCE SAS	TAS	France
9	CBRNE Ltd	CBR	United Kingdom

Table 1: ULTIMATE consortium partners

ULTIMATE will pioneer the development of industrial-grade hybrid Artificial Intelligence (AI) that forms a critical foundation for the adoption of AI in industry. The industrial-grade hybrid AI will be developed in three stages to ensure trustworthiness:

- 1st stage: relying on interdisciplinary data sources and adhering to physical constraints;
- 2nd stage: development of tools for explaining, evaluating and validating hybrid AI algorithms and asserting their adherence to ethical and legal regulations;
- 3rd stage: these will be exemplified using real-world industrial use cases in the Robotic (collaboration between human and robots for logistics activities) and Space domains (Failure detection for satellites) to promote the widespread adoption of hybrid AI in industry.

Any breakthrough generic hybrid AI architectures with improved explainability and interpretability, and the predictive model on trustworthiness developed in ULTIMATE will provide industrial organisations with improved shopfloor efficiency (i.e. reduction of downtime by 30% and associated operational costs). This will empower their staff through trustworthy human/machine cooperation, allowing highly skilled jobs and increasing decision power and safety. This will be beneficial to European industry to gain pre-emptive advantage in the market of industrial AI solutions and will eventually increase trustworthiness in the use of hybrid AI components by the wider general public.

To develop the ULTIMATE hybrid AI algorithms and solutions, the technical partners will use specific domain knowledge and massive amounts of heterogeneous technical sensory data. The datasets will be provided by the Use Case (UC) Owners. No personal data are collected or used for the development and implementation of hybrid-AI algorithms and solutions. The visual AI solutions (WP3) are limited in scope to object recognition for picking up articles and placing them. The biometric recognition will be disabled within the component.

The ULTIMATE hybrid AI algorithms and solutions will be demonstrated within three Use Cases (UCs):

- UC1 (Space): TAS – TAI-based Failure Detection, Isolation and Recovery (FDIR) for Satellite on-board autonomy. Preventive on-board failure monitoring and prognostics, on-board preventive management of failures by promoting and facilitating predictive and prescriptive maintenance (while keeping human in the loop).
- UC2 (Robotic workshop): PIAP – Manufacturing workstation with mobile robots (Automated Guided Vehicle, AGV), e.g., warehouses. Enhancement of human operators in their tasks, boosted production performance.
- UC3 (Industry): ROB – Robot manipulator (robotic arms). Time and cost reduction for multiple object detection and manipulation with the same mobile manipulator in logistic environments.

1.2. Structure of the document

The technical and organisational measures described in this deliverable aim to protect the rights of the workers involved in UC2 (Robotic Workshop) and UC3 (Industry – Robotic Arm) demonstrators as they include the detection and precise tracking of the human workers.
The UC1 (Space) uses only sensory data, no human worker is involved in the demonstrator.

Section 2 of the deliverable offers the argument that a Data Protection Impact Assessment does not need to be conducted, based on the requirements and the guidance provided by GDPR and consulting normative sources.

Section 3 of the document describes the technical and organisational measures which are implemented in ULTIMATE in order to protect the privacy and data protection rights of data subjects and research participants in WP5 Demonstrators: UC2 - Robotic workshop (PIAP) and UC3 – Industry: Robotic arms (ROB), including compliance statements of PIAP and ROB DPO's and the support and approval letter from the External Ethical Expert (attached in the annex 5).

2. Data Protection Impact Assessment

2.1. Normative and legal definitions

One of the obligations that the General Data Protection Regulation (GDPR)[1] places upon controllers under certain circumstances is to carry out a DPIA, which is aimed at identifying the risks to the rights and freedoms of natural persons caused by certain types of processing, especially those that are new.

Article 35 GDPR states that:

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.
[…]
A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da. (27th de April de 2016

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(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or a systematic monitoring of a publicly accessible area on a large scale.*

The article is not particularly clear, which makes it advisable to consult other sources. The Information Commissioner's Office (ICO)[2] published an online checklist aimed at assisting organisations in assessing whether carrying out a DPIA is mandatory. We have underlined in the text the criteria applying to ULTIMATE.

Consideration to carry out a DPIA is advised for the following activities:

- evaluation or scoring;
- automated decision-making with significant effects;
- systematic monitoring;
- processing of sensitive data or data of a highly personal nature;
- processing on a large scale;
- processing of data concerning vulnerable data subjects;
- innovative technological or organisational solutions;
- processing that involves preventing data subjects from exercising a right or using a service or contract.

Based on the above, carrying out a DPIA is mandatory if it is foreseen to:

- use systematic and extensive profiling or automated decision-making to make significant decisions about people;
- process special-category data or criminal-offence data on a large scale;
- systematically monitor a publicly accessible place on a large scale;
- use innovative technology in combination with any of the criteria in the European guidelines;
- use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.
- carry out profiling on a large scale;
- process biometric or genetic data in combination with any of the criteria in the European guidelines;
- combine, compare or match data from multiple sources;
- process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines;
- process personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;
- process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;
- process personal data that could result in a risk of physical harm in the event of a security breach.

2.2. Analysis of DPIA requirements in WP5 demonstrators

The situations that apply to ULTIMATE WP5 UC2 and UC3 demonstrators are in the context of using innovative technological solutions (hybrid AI) which process personal data in ways that involves tracking individuals' behaviour (workers interacting with robots in the robotic workshop, in the case of UC2, and workers interacting with the robotic arm, in the case of UC3.

[2] Information Commissioner's Office, Data Protection Impact Assessment Check List, available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-impact-assessments/

However, none of these activities are done in combination with the criteria mentioned in the European legislation: the UC2 and UC3 demonstrators are not aimed at profiling individuals and none will lead to significant decision about individuals. They are done in the context of research and innovation activities involving a small number of workers.

We conclude that a DPIA is not necessary to be conducted in the context of WP5 UC2 and UC3 Demonstrators.

3. Overcoming barriers to tracking individual behaviour research ethics requirements: technical and organisational measures within ULTIMATE consortium

This section will describe mechanisms for addressing ethics requirements related to data management following principles behind the above risk assessment conducted within the DPIA as defined in the Article 35 GDPR. This analysis is also based on requirements reflected in D1.3 Data Management Plan and Research Ethics. Data protection issues resulting in a high risk to individuals go beyond the ones to be screened regarding DPIAs, which include the amount and sensitives of collected personal identifiers or individual tracking. As explained above, although the analysis of UC2 and UC3 demonstrators and the examination of proportionality in the data processing doesn't call for a DPIA to be conducted, it is important to establish safety technical and organisational measures for personal data processing.

3.1. Technical measures

Article 32 GDPR establishes the obligation to guarantee an appropriate level of security according to the state of the art.

Article 32

1. *Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
    a. *the pseudonymisation and encryption of personal data;*
    b. *the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;*
    c. *the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
    d. *a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.*

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

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

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

Technical measures can be used to protect personal data from misuse or abuse. These include anonymisation and pseudonymisation, encryption and restricted access control. All of them are used within ULTIMATE and are described below.

3.1.1. Anonymisation and pseudonymisation

Anonymisation and pseudonymisation are both defined in the GDPR with the aim of making compatible the processing of data for reasonable and legitimate processing activities and the protection of the fundamental rights to privacy and data protection. Both pseudonymised data and anonymous data are defined in recital 26 as follows (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 (GDPR).

Anonymised (anonymous) data:

The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

Pseudonymised data:

Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.

From these definitions, it is inferred that pseudonymisation does not take away the personal nature of the data, which means that data can still be linked to specific individuals. The criteria used to determine if a data set has been pseudonymised is subject to interpretation and has a contextual nature; it depends on the nature of the data and what means are considered to be reasonable to protect that data, as well as the means required to re-identify the natural person.

The Article 29 Working Group[3] published an important opinion paper that attempted to provide some clarification regarding the distinction between anonymisation and pseudonymisation, which reads the following: *Pseudonymisation is not a method of anonymisation. It merely reduces the link-ability of a dataset with the original identity of a data subject, and is accordingly a useful security measure.*

[3]Article 29 Working Party (10th of April 2014). Opinion 05/2014 on Anonymisation Techniques, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

3.1.2. Encryption

Encryption[4] refers to the procedure that converts clear text into a hashed code using a key, where the outgoing information only becomes readable again by using the correct key. This minimises the risk of an incident during data processing, as encrypted contents are basically unreadable for third parties who do not have the correct key. Encryption is the best way to protect data during transfer and one way to secure stored personal data. It also reduces the risk of abuse within an organisation, as access is limited only to authorised people with the right key.

The GDPR also recognizes the risks when processing personal data and places the responsibility on the controller and the processor in Art. 32(1) to implement appropriate technical and organisational measures to secure personal data. The GDPR deliberately does not define which specific technical and organisational measures are considered suitable in each case, in order to accommodate individual factors.

3.1.3. Restricted access control

Access control system is a way to ensure access to assets is authorized and restricted based on business and security requirements (ISO/IEC 27000, Integrating Access Control and Business Process for GDPR Compliance 20184)[5]. Access Control ensures only the intended people can access security classified data and these intended users are only given the level of access required to accomplish their tasks. It is also considered as a fundamental building block for secure information sharing.

3.2. Organisational measures

3.2.1. Informed consent procedures

Research activities carried out within WP5, Use Case 2 Robotic workshops demonstrator (PIAP) and Use case 3 Industry - Robotic arm demonstrator (ROB) will involve human participants. Their personal data will be processed on the basis that they have been explained the tasks at hand and were made aware of their rights through an information sheet and explanation by researchers, after which they must provide their consent in a consent form to participate. D1.3 describes these procedures in detail and includes templates of the consent forms to be used as annexes (section 2.5 Research ethics Protocol).

Informed consent: the legal basis

The definition of consent outlined when using consent as the lawful basis for processing personal data has been refined in the Regulation as: "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". (GDPR, Article 4).

The lawful basis for consent to participation in research and for the personal data collection and processing is GDPR Article 6(1) and Article 9.2

- *GDPR Article 6(1) (e) "Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested the controller".*
- GDPR Article 9(2) (j) "*Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject*".

Informed consent: good practice general guidance

The following outlines some of the good practice considerations for obtaining and processing personal

[4] Article 29 Working Party Statement of Privacy available at https://ec.europa.eu/newsroom/article29/items/622229/en

[5] Sharron M., The Ultimate Guide to GDPR Compliance with ISO 27001 and ISO 2770, available at https://www.isms.online/general-data-protection-regulation-gdpr/the-ultimate-guide-to-gdpr-compliance-with-iso-27001-and-iso-27701/

data through informed consent:

- Consent should be a positive opt-in;
- Explicit consent requires a very clear and specific statement of consent in words, rather than by any other positive action;
- Avoid making consent to processing a precondition of any service you are offering;
- Keep evidence of consent – who, when, how, and what;
- Participant consent forms should be stored securely and confidentially;

The participant information sheet and consent forms should:

- Outline the lawful basis, 'public task', on which the project ULTIMATE processes personal data (and the condition for processing if sensitive data is collected);
- Be specific and granular where possible to get separate consent for separate things;
- Explain why Project ULTIMATE wants the data (purpose), and will do with it (intended use), and how long the data will be stored;
- Explain who, if anyone, the data will be shared with; and in what format the data will be shared;
- Highlight what it is done to ensure the security of personal information;
- Be clear, concise, user friendly;
- Make it easy for people to withdraw consent to participate in research and tell them how they can withdraw their participation (explaining any limitations to withdrawing or deleting their data);
- Explain that the participant has the right to complain to the Project ULTIMATE management team and the ULTIMATE PEO if they are unhappy with the data management;
- Contain the contact details of the principal researcher and the Project ULTIMATE Data Protection Officer.

Rights of data subjects

Data subjects have the following rights:

- to obtain a confirmation whether or not their data are processed, and information on the categories of data being processed, in what ways, and for what purposes as well as the recipients or categories of recipients to whom the data are disclosed;
- to assure rectification of inaccurate or incomplete personal data;
- to block the processing of data for which the data subjects contest the accuracy, until accuracy is checked;
- participants will be free to withdraw at any time without justification, and their data will be deleted (if not already anonymous) as per the processes described previously.

Consent forms: handling rules

When involved in the handling of consent forms, PIAP and ROB project members must apply the following rules:

- use the consent form and information sheet templates documented in D1.3 and the related annexes;
- release a new/updated consent form, when changing study procedures and/or identifying new risks to participants;
- obtain PEO approval before using a revised consent form through the use of the Research Ethics Protocol;
- keep all original signed consent forms with research study records in a secure place and manner;
- verify each participant is given a signed and dated copy of the consent form at the time of initial consent;
- verify participants answer all questions on the consent form;
- verify the person obtaining consent (principal research) has signed, when applicable;
- verify signers complete all applicable lines on the consent form;
- verify participant enters the date of signing at the time of consent.

PIAP and ROB project members must <u>not</u>:

- use expired consent forms;
- alter approved consent forms
- leave consent form questions incomplete;
- confuse initials with check marks;
- share consent forms with non-authorised persons;
- include consent instructions not easy to follow, as they might be considered as noncompliance.

3.2.2. Governance and security

Data Management Plan

A policy has been put in place concerning data processes, to ensure these follow the principles set by the GDPR. To this effect, a Data Management Plan (DMP) was created as part of D1.3, to guide consortium members. This DMP gives a summary of the data collected during the project and sets out the guidelines to be followed by the consortium members. Changes and development to the data management plan will be reflected in the DMP as established in the GA. The consortium members were asked about the personal data they collect and about the security measures implemented in order to safeguard them. These specific measures will be explained in D1.3.

UC Owners nominated DPOs

In addition to that, Each Use Case Owner (TAS, ROB, PIAP) has appointed a DPO in order to further guarantee the data subject's rights.

- UC1 Space (TAS): Evelyn Truls-Pellegrino
- UC2 Robotic workshop (PIAP): Agnieszka Sprońska
- UC3 Industry (ROB): Nuria Pla

Their responsibilities are presented in D1.3.

UC Owners DPOs Compliance Statement

In order to comply with the ethics requirement, the ULTIMATE Project Ethics Officer has asked the ULTIMATE Robotic Use Case Owners (ROB and PIAP) to determine whether provisions of national data protection laws require them to notify and consult their data protection authorities or obtain further authorization for the personal data processing activities during the hybrid AI demonstration in WP5.

While the GDPR has removed the general duty of notification introduced under Directive 95/46 EC, article 36.5 of the Regulation allowing member states to nevertheless require data controllers to consult with, and obtain prior authorization from data protection authorities when this processing occurs for the performance of certain tasks.

In order to fulfil this requirement, the data protection officers or legal departments of the ULTIMATE Robotic Use Case (UC) Owners (ROB and PIAP) involved in the processing of personal data have been tasked with ascertaining whether such a prior consultation is necessary under national law and, if need be, contacting their data protection authority for this purpose.

As a result of the consultation, both PIAP and ROB have assessed this matter and concluded that there exist no national legal provisions in Poland and Spain requiring their organization to contact the relevant data protection authority for further consultation or authorization. As such, the European Commission's condition in D7.1 shall be fulfilled by obtaining a statement of compliance by our data protection officer and keeping it on file. The ROB and PIAP compliance statements are attached as annexes (annex no 1 and annex no 2) to this deliverable.

External Ethics Adviser approval letter

The European Commission Requirement for the WP5 mentions that the external ethics advisor should ensure the rights of the workers are preserved concerning privacy and data protection and that they are truly free to accept or reject participation to the UC2 and UC3 Demonstrators in WP5.

In order to comply with these requirements, the ULTIMATE Project Ethics Officer (PEO) has asked the External Ethics Advisor to review the deliverables setting the relevant policies for the WP5 Demonstrator activity (D1.3 Data Management Plan and Research Ethics) and the present document D7.1 Ethics requirement no 1., and to offer advice and suggestions.
As a result of this collaboration the EEA has approved all the relevant policies and related documentation. The approval letter is attached as annex to this document (annex no 3.)

3.2.3. Training

The importance of training comes from the fact that it ensures that research participants are adequately informed of all aspects required in Article 13 GDPR, as well as what is proportionate and recommended for them to know. Thus, it empowers research subjects, which in turn reinforces compliance with the principle of accountability. Partners have trained their teams on data protection matters internally and are receiving continuous training as part of T1.5, which is intended to help them detect and tackle privacy and ethical issues during the design and deployment of the UC2 and UC3 demonstrators in WP5 (T5.1).

3.2.4. Technical and organisational measures adopted by ULTIMATE

The technical and organisational measures adopted by the ULTIMATE project are summarised in the following table:

	PIAP	ROB	TRT
Informed consent	Research ethics protocol procedures will be followed and informed consent will be collected for all the participants in the WP5 UC2 Demonstrator	Research ethics protocol procedures will be followed and informed consent will be collected for all the participants in the WP5 UC3 Demonstrator	Not applicable
DPOs	In place	In place	In place
DPOs Compliance Statement	Submitted (see annex 1)	Submitted (see annex 2)	Not applicable
EEA approval letter	Not applicable	Not applicable	Obtain (see annex 3)
Training	Offered by the PEO during Ethics Workshop on 3rd of April 2023 and offered as continuous guidance under T5.1	Offered by the PEO during Ethics Workshop on 3rd of April 2023 and offered as continuous guidance under T5.1	Offered by DPO during the kick off meeting 27th of October 2023 and offered as continuous guidance under T5.1
Anonymisation and pseudonymisation	If needed, face blurring will be applied to the camera data to anonymise the dataset	Use of a custom ROS package to blur faces that are detected using a trained Neuronal Network	No supplementary measure
Encryption	Encryption ensured by the Cryptobox tool	Encryption ensured by the Cryptobox tool	Encryption natively ensured by the Cryptobox tool (transfers of data-sets between partners)
Restricted access control	Login/password	Login/password	Login / password

Table 2. Technical measures in relevant partner organisations.

4. Summary and Conclusions

The D7.1 elaborates on the ethical requirements imposed by the EU Commission on the ULTIMATE project as part of the Grant Agreement 101070162: "Hybrid AI for Robotic navigation and collaborative work" demonstrator considers the detection and precise tracking of the human workers. The ethics advisor should ensure that the rights of the workers are preserved concerning privacy and data protection and that they are truly free to accept or reject participation to the research experiment. A first report on this topic should be provided before the start of WP5 (M12)".

Section 1 of the document introduces the project ULTIMATE and describes the Use Cases Demonstrators in WP5 which involve participation of workers in the research experiment: UC2 - Robotic workshop (PIAP) and UC3 – Industry: Robotic arms (ROB).

In the section 2 we have conducted an analysis of the GDPR and the normative documents offering the argument that a Data Protection Impact Assessment (DPIA) doesn't need to be conducted.

Section 3 the document describes the technical and organisational measures which are implemented in ULTIMATE in order to protect the privacy and data protection rights of data subjects and research participants in WP5 Demonstrators:

- Technical measures: Anonymisation and Pseudo-anonymisation; Encryption, Restricted Access.
- Organisational measures: Informed Consent, Nomination of DPOs; DPOs' Compliance Statements, Training, and External Ethics Adviser Approval Letter.

In the annex 5 we have attached the compliance statements of PIAP and ROB DPOs and the support and approval letter from the ULTIMATE External Ethical Advisor.

The project coordinator, TRT, has overall responsibility of the implementations of these measures with support from Project Ethics Officer (PEO) from CBR and under the guidance of the External Ethics Advisor.

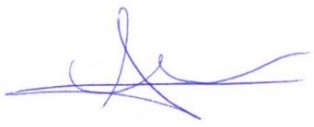
5. Annex

5.1. Robotnik Data Protection Officer Compliance Statement

This document has been submitted for the purpose of meeting the ethical requirements imposed on Robotnik as part of the European Union Horizon Europe project ULTIMATE (Grant Agreement 101070162). These ethical requirements were provided by the European Commission after the approval of the project's funding. They are reflected in the ULTIMATE Grant Agreement and final version of the Division of Work. As a section of Work Package 7 ("Ethics Requirements"), the consortium must hereon draft and submit Deliverable 7.1 ("Requirement No.1"). The European Commission has defined the work under this Deliverable as follows:
The "Hybrid AI for Robotic navigation and collaborative work" demonstrator considers the detection and precise tracking of human workers. The ethics advisor should ensure that the rights of the workers are preserved concerning privacy and data protection and that they are truly free to accept or reject participation on the research experiment. A first report on this topic should be provided before the start of WP5 (meaning M12)"

In order to comply with the ethics requirement, the ULTIMATE Project Ethics Officer has asked the ULTIMATE Robotic Use Case Owners (ROB and PIAP) to determine whether provisions of national data protection laws require them to notify and consult their data protection authorities or obtain further authorization for the personal data processing activities during the hybrid AI demonstration in WP5. While the GDPR has removed the general duty of notification that was introduced under Directive 95/46 EC, article 36.5 of the Regulation allows member states to nevertheless require data controllers to consult with, and obtain prior authorization from, data protection authorities when this processing occurs for the performance of certain tasks. In order to fulfil this requirement, the data protection officers or legal departments of the ULTIMATE Robotic Use Case (UC) Owners (ROB and PIAP) involved in the processing of personal data have been tasked with ascertaining whether such a prior consultation is necessary under national law and, if need be, contacting their data protection authority for this purpose.
This document reflects that Robotnik has assessed this matter and concluded that there exist no national legal provisions in Spain requiring our organization to contact the relevant data protection authority for further consultation or authorization. As such, the European Commission's condition in D7.1 shall be fulfilled by obtaining a statement of compliance by our data protection officer and keeping it on file. This document contains this statement below.

As the designated data protection officer (DPO) for Robotnik in project ULTIMATE, I, Nuria Pla hereby confirm that all personal data collection and processing within WP5 Robotnik Robotic Use Case demonstration will be carried out according to EU and national legislation and following the data management procedures agreed within ULTIMATE project (*D1.3 Data Management Plan and Research Ethics*). The GDPR and the national laws implementing the Regulation shall be adhered to during WP5 Robotnik Robotic Use Case demonstration and while collecting, managing, using and deleting personal data of the participants.



Signed Name
Date 27/09/2023
Email: npla@robotnik.es

5.2. PIAP-Lukasiewicz Data Protection Officer Compliance Statement

This document has been submitted for the purpose of meeting the ethical requirements imposed on Łukasiewicz-PIAP as part of the European Union Horizon Europe project ULTIMATE (Grant Agreement 101070162). These ethical requirements were provided by the European Commission after the approval of the project's funding. They are reflected in the ULTIMATE Grant Agreement and final version of the Division of Work. As a section of Work Package 7 ("Ethics Requirements"), the consortium must hereon draft and submit Deliverable 7.1 ("Requirement No.1"). The European Commission has defined the work under this Deliverable as follows:
The "Hybrid AI for Robotic navigation and collaborative work" demonstrator considers the detection and precise tracking of human workers. The ethics advisor should ensure that the rights of the workers are preserved concerning privacy and data protection and that they are truly free to accept or reject participation on the research experiment. A first report on this topic should be provided before the start of WP5 (meaning M12)"

In order to comply with the ethics requirement, the ULTIMATE Project Ethics Officer has asked the ULTIMATE Robotic Use Case Owners (ROB and PIAP) to determine whether provisions of national data protection laws require them to notify and consult their data protection authorities or obtain further authorization for the personal data processing activities during the hybrid AI demonstration in WP5. While the GDPR has removed the general duty of notification that was introduced under Directive 95/46 EC, article 36.5 of the Regulation allows member states to nevertheless require data controllers to consult with, and obtain prior authorization from, data protection authorities when this processing occurs for the performance of certain tasks. In order to fulfil this requirement, the data protection officers or legal departments of the ULTIMATE Robotic Use Case (UC) Owners (ROB and PIAP) involved in the processing of personal data have been tasked with ascertaining whether such a prior consultation is necessary under national law and, if need be, contacting their data protection authority for this purpose. This document reflects that Łukasiewicz-PIAP has assessed this matter and concluded that there exists no national legal provisions in Poland requiring our organization to contact the relevant data protection authority for further consultation or authorization. As such, the European Commission's condition in D7.1 shall be fulfilled by obtaining a statement of compliance by our data protection officer and keeping it on file. This document contains this statement below.

As the designated data protection officer (DPO) for Łukasiewicz-PIAP in project ULTIMATE, I, Agnieszka Sprońska hereby confirm that all personal data collection and processing within WP5 Łukasiewicz-PIAP Robotic Use Case demonstration will be carried out according to EU and national legislation and following the data management procedures agreed within ULTIMATE project (*D1.3 Data Management Plan and Research Ethics*). The GDPR and the national laws implementing the Regulation shall be adhered to during WP5 Łukasiewicz-PIAP Robotic Use Case demonstration and while collecting, managing, using and deleting personal data of the participants.

Signed 

Name Agnieszka Sprońska

Date 24/07/2023

Email: agnieszka.spronska@piap.lukasiewicz.gov.pl

5.3. External Ethics Adviser support and approval letter

As independent External Ethics Advisor on the ULTIMATE (101070162) project, I have had the opportunity to review the development of the "Data Management Plan and Research Ethics and Guidelines Protocol" (Deliverable 1.3) that was submitted on 31/01/2023.

I proof read the Plan with great care and I considered it to be a very thorough, detailed and comprehensive description of the data management procedures that will be implemented to ensure the compliance of the research activities of ULTIMATE with the standards, guidelines and regulations of Horizon Europe and is in compliance with the General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 and with relevant National Legislations.

I recommended some relatively minor modifications, which were accepted and implemented.

I indicated my approval of the Deliverable 1.3.

I have recently received a final draft for review of the Report on Deliverable D 7.1: "Requirement No. 1 Ethics". This is a response to an Ethics Requirement included in the Grant Agreement (101070162). This requires that "The ethics advisor should ensure that the rights of the workers are preserved concerning privacy and data protection and that they are truly free to accept or reject participation to the research experiment in WP5". The response is due for submission on 30/09/2023 and prior to the commencement of WP5 in Month 12.

The response is divided into 3 sections:

Section 1 describes the studies in WP5, which includes the participation of workers involved in UC2 (Robotic Workshop) and UC3 (Industry – Robotic Arm) demonstrators. These studies include the detection and precise tracking of the workers.
It should be noted that UC1 (Space) uses only sensory data, and no human workers are involved in the demonstrator.

Section 2 provides a thorough explanation that a Data Protection Impact Assessment (DPIA) does not need to be carried out, based on the requirements and the guidance provided by the GDPR and consulting normative sources.

Section 3 provides details of the technical and organisational measures that will be implemented to protect the privacy and data protection rights of data subjects and research participants in WP5 Demonstrators. This Section includes statements from the relevant DPOs indicating their opinion that all personal data collection and processing within WP5 will comply with EU and national legislation. They confirm that the GDPR and the national laws implementing the Regulation will be adhered to during WP5. This Section also includes this letter of approval from the External Ethics Advisor.

The Consortium has provided detailed guidance on the procedures that will be implemented to ensure the fully informed consent of any workers participating as volunteers in WP5. These procedures are described in D1.3 and include templates of the Informed Consent Forms to be used. The information sheets that will accompany the Informed Consent Forms are very comprehensive and cover all the relevant issues that must be explained to potential participants before deciding whether or not to sign the consent form. It will be made clear that they can withdraw consent to participate in the research at any stage can may withdraw or delete their data. They will be assured that has the right to complain to the ULTIMATE management team, the DPOs and the Project Ethics Officer and relevant contact details will be provided.

It is my opinion that these procedures, are sufficiently rigorous to ensure that the workers who are recruited to take part in the real world industrial Use Cases will be appropriately informed about their rights when participating in the research and the technical and organisational measures that will be implemented to protect their privacy and data protection rights. They will also be informed about the use of Artificial Intelligence (AI) technology in these studies. With the implementation of the procedures described in D7.1, I am confident that the workers will be fully informed and free to accept or reject participation to the research experiment in WP5

Overall, I am satisfied that the Ethics Requirement described in the Grant Agreement has been satisfied and I approve the Report.

Signed:

Name: James A Houghton

Place: Galway, Ireland.

E Mail: jim.houghton@nuigalway.ie

Date: 30/09/2023